VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky

DIPLOMOVÁ PRÁCE

Ostrava 2009 Bc. Antonín HLOSTA

VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Systém pro evidenci personální a mzdové agendy
System for Personal and Salary Evidence

Ostrava 2009 Bc. Antonín HLOSTA

==========ZADÁNÍ DIP.PRÁCE==========

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 7.května 2009 Bc. Antonín HLOSTA

Poděkování

Děkuji Ing. Radoslavovi Fasugovi za odborné vedení práce a mnoho cenných rad a podnětů.

Abstrakt a klíčová slova

Abstrakt:

Hlavní zaměření diplomové práce je na problematiku tvorby systému pro mzdovou a personální agendu. Práce se zabývá problematikou výpočtů mezd a vysvětlení základních zákonů ze zákoníku práce. Dále se práce zabývá bezpečností pro tvorby různorodých informačních systémů. V rámci diplomové práce je také návrh a implementace informačního systému pro mzdovou a personální agendu. Informační systém je navržen v prostředí internetu a měl by sloužit pro outsourcing mzdového účetnictví. Základem je sběr firemní, personální a mzdové agendy. Dále je kladen důraz na výpočet náhrad ze mzdy a mezd. Také byla naimplementována komponenta pro elektronické zadávání úkolového listu. Práce obsahuje popis funkcí, podrobnou datovou a funkční analýzu. Implementace v prostředí Windows s podporou SQL databázového serveru.

Klíčová slova:

analýza, autentizace, autorizace, autorizace, bezpečnost, daně, datová analýza, datový slovník, DFD diagram, ER diagram, funkční analýza, implementace, informační systém, návrh, mzda, mzdová agenda, mzdové účetnictví, náhrada mzdy, návrh implementace, outsourcing, personální agenda, platba, sociální pojištění, úkolový list, výpočet mezd, zákoník práce, zdravotní pojištění

Abstract and key words

Abstract:

This thesis is focused on building an information system for personal and salary evidence. The scope of the work is salary accounting and demonstrativ of the basic laws of the Labour Code. Further scope of the work is security for building the difference of the Information Systems. Within this thesis are an Information System design and implementation for personal and salary evidence. An information system is projected for internet medium and the system work as outsourcing for wages accounting. The basis of this work is requirement specification information for company, personal and salary evidence. Further basis is location accent on calculation remund of wages and wages. Information system have implemented work sheet component for electronic insert data. This work also contains product functions description with detailed data and functional analysis. It is implementation in Windows operation System with SQL database server usage support.

Key words:

analyse, authentication, authorization, security, taxes, data analyse, data dictionary, DFD diagram, ER diagram, functional analyse, implementation, information system, wages, salary evidence, wages accounting, remund of wages, implementation design, outsourcing, personal evidence, payment, social instance, work sheet, calculation wages, labour code, health instance

Seznam použitých symbolů a zkratek

Poznámka: zkratka je vysvětlena vždy u prvního výskytu v poznámce pod čárou. Výskyty zkratek ZP a Kč nejsou v seznamu pro velký výskyt zaznamenávány.

Obsah

1 Úvod

Pečovat o zaměstnance a celá řada činností s tím souvisejících jsou v dnešní době náročným úkolem v každé společnosti. Pro zjednodušení náročnosti mzdové a personální agendy a prokazatelného snížení nákladů, lidé vyhledávají informační systémy podporující tuto problematiku. Mzda pro nás představuje odměnu za provedenou práci v pracovně právním vztahu a je vyplácena ve výplatních termínech, zpravidla zpětně za provedenou práci. V minulosti se mzda vyplácela v předem dohodnuté výši jako jednopoložková částka. Prvním významným dokumentem, který se zabýval problematikou pracovně právních vztahů, byl horní zákoník Václava II z let 1300-1305. Od této doby vývoj neustále pokračuje. Mzda se začala skládat z několika složek (základní mzda, náhrada mzdy a výkonnostní složky mzdy), je možné také plnění peněžité hodnoty, tzv. naturální mzda a na mzdu se také vztahují povinné odvody, dobrovolné odvody, srážky, exekuce a další. To všechno mělo vliv pro vývoj informačních systému a výpočet mezd. Tyto systémy jsou dále propojené z další řádkou systémů, jako jsou účetní systémy, bankovní systémy a podobně.

Ve složitosti výpočtů mezd je čím poměrně komplikované se orientovat. Při výpočtu mezd bez podpůrných programů se jen stěží obejdeme. V dnešní době rozvoje služeb poskytovaných prostřednictvím internetu, jsem se rozhodl prozkoumat tuto oblast poskytování mzdového účetnictví přes internet. V současnosti je celá řada profesionálních i poloprofesionálních softwarů[1] pro výpočet mezd. Tyto systémy jsou na bázi stolních programů a mohou být pro určitou skupinu firem nákladné. Outsourcing[2] mzdového účetnictví prostřednictví internetu je v počátcích svého rozvoje. Proto, jsem se rozhodl pro diplomovou práci vybrat a zpracovat toto téma zabývající se mzdovou a personální agendou a vytvoření webové aplikace, která by poskytla outsourcing mzdového účetnictví pro malé a střední firmy.

1.1 Současný stav

Současný trh se systémy pro správu mezd by se dal rozdělit do tří skupin. První skupinou by mohly být lokání aplikace. S programy pro zpracování mezd se budu více zabývat v 6. kapitole. Většina těchto aplikací je budována v delším časovém rozpětí. Jejich další rozšiřování spočívá spíše v implementování nových platných změn v legislativě mezd a přizpůsobení běhu aplikace pro nové operační systémy.

Na straně internetových informačních systémů už je nabídka podstatně chudší. Do této druhé skupiny spadají firmy, které nenabízejí svůj implementovaný software, ale nabízejí pouze

[1] Software – programové vybavení

[2] Outsourcing – nákup služeb mimo podnik

informační službu svého implementovaného informačního systému pro mzdovou a personální agendu v prostředí internetu. Myšlenkou je poskytnout systém pro výpočet mezd jako služby pro menší a střední firmy, kde přihlášená firma (osoba) zadá personální a mzdové údaje pro své pracovníky. Následně za poplatek si nechá vypočítat mzdy, odvody, vytiskne tiskové sestavy a podobně. Tento systém na základě zadaných údajů samostatně vypočítá potřebné údaje a sestaví potřebné výstupy.

Do druhé skupiny nelze zahrnovat firmy, které nabízí zpracování mezd na zakázku. Tyto firmy spadají do třetí skupiny. Firmy v této skupině používají převážně stolní aplikace pro mzdovou a personální agendu.

2 Mzdy

Legislativou okolo mezd v ČR[3] se zabývá zákoník práce – zákon č.262/2006 Sb. Zákoník práce je sbírka zákonů, které se zabývají pracovně právními vztahy. Zákoník práce slouží pro vymezení práv mezi zaměstnavateli a zaměstnanci. Tento zákoník slouží pro zaměstnance i zaměstnavatele zároveň. Zaměstnanec zde hledá práva, které mu náleží a snaží se tato práva prosadit u zaměstnavatele. Pokud ale není zaměstnavatel spokojen s prací nebo chováním svých zaměstnanců, může využít těchto zákonů ve svůj prospěch vůči zaměstnanci.

Při nástupu zaměstnance do zaměstnání, zaměstnanec podepisuje smlouvu, kde jsou zanesena jeho práva a povinnosti. Pokud některé situace nejsou usnesené v pracovní smlouvě, pak se tyto situace řídí právě dle zákoníku práce.

V této kapitole je uveden jen výtah důležitých části zákoníku práce s příklady. Tato kapitola slouží pro základní orientaci v problematice mezd a neklade si za cíl podat vyčerpávající informace ve mzdové problematice. Kapitola se také nezabývá např. mzdovou problematikou studentů.

Další zákony upravující mzdové a platové předpisy jsou:

- Zákon č. 143/1992 Sb. zákon o platu
- Zákon č. 118/2000 Sb. zákon o ochraně zaměstnanců při platební neschopnosti zaměstnavatele a o změně některých zákonů
- Nařízení vlády č. 469/2002 Sb. nařízení vlády, kterým se stanoví katalog prací a kvalifikační předpoklady a kterým se mění nařízení vlády o platových poměrech zaměstnanců ve veřejných službách a správě
- Nařízení vlády č. 567/2006 Sb. nařízení vlády o minimální mzdě, o nejnižších úrovních zaručené mzdy, o vymezení ztíženého pracovního prostředí a o výši příplatku ke mzdě za práci ve ztíženém pracovním prostředí

Případná použití dalších zákonů pro mzdovou potřebu budou uvedena v jednotlivých kapitolách.

Informace pro tuto kapitolu jsem čerpal z několika zdrojů. Pro orientaci v zákonech, nařízení vlády, vyhláškách a jiné právní normy jsem použil zákony na internetu na stránkách Ministerstva vnitra České republiky[10], internetové stránky business.center.cz [12] nebo internetové stránky podnikatel.cz [11]. Internetové stránky měšec.cz [16] jsem využíval pro informace o daních, sociální a zdravotní pojištění, mzdové tabulky. Informace o nezabavitelné částce a daních jsem čerpal z internetových stránek businessInfo.cz [17]. Pro orientaci ve

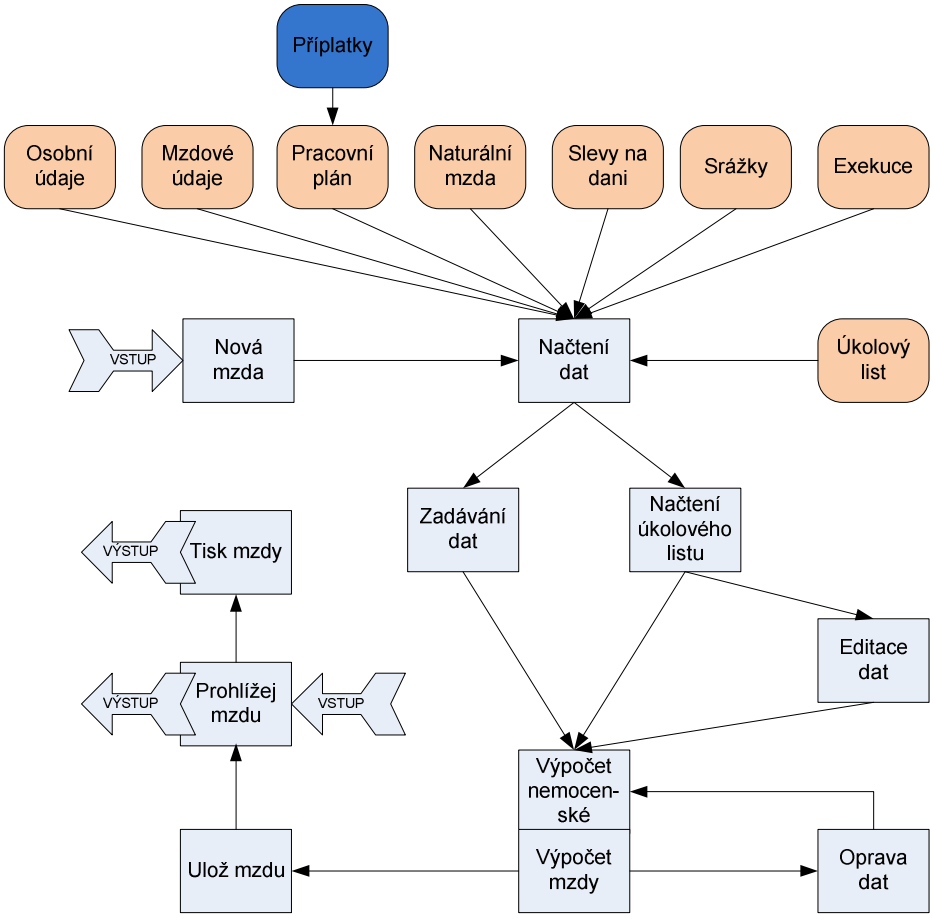
[3] ČR – Česká republika

mzdové problematice jsem také využil finance.cz [18] a server Výplata [19]. Pro historii odměňování práce jsem využil internetových zdrojů na stránkách Ministerstva práce a sociálních věcí [13], Rovné šance [14], Dějepis.com[20] nebo z kroniky Bílý Újezd [15].

Jednotlivé podkapitoly většinou obsahují vzorový příklad. Řešení těchto příkladů nelze považovat ze všeobecné, i když je obecně popsané. Řešení je určeno vždy pro konkrétní vzorový příklad. Pokud by došlo k jiné specifikaci vzorového příkladu, řešení se může měnit. Zkratky použité ve vzorových příkladech jsou definované pouze pro tyto vzorové příklady. Zkratky jsou vysvětlené v poznámce pod čarou u prvního výskytu. Další výskyty zkratek jsou zaznamenané v rejstříku zkratek v sekci *vzorové příklady*. Pokud je zkratka použitá v teoretickém textu, pak zkratka se nachází v rejstříku mimo oblast *vzorové příklady*.

Pokud dochází k implicitnímu zaokrouhlování ve vzorových příkladech, zaokrouhluje se podle zákona na celé koruny směrem nahoru. Základ daně se zaokrouhluje na celé stokoruny nahoru. Další zaokrouhlování je uvedeno v příslušných podkapitolách.

Výpočet mzdy by se měl skládat z několika kroků. Po informační systém na výpočet mezd byl vytvořen následující diagram.



Obrázek 1: Výpočet mezd

Vstupem do výpočtu mzdy je událost “Nová mzda“. Po výpočtu mzdy lze z procesu vypočet vystoupit v události “Prohlížej mzdu“ (nastane hned po uložení mzdy) nebo po tisku mzdového listu v události “Tisk mzdy“. Pokud je mzda vypočtená, lze ji následně prohlížet a tisknout. Pro prohlížení už předem vypočtené mzdy lze vstoupit přímo do události “Prohlížej mzdu“. Proces (průchod diagramem) lze kdykoliv ukončit bez uložení v událostech “Zadávání dat“, “Načtení úkolového listu“, “Editace dat“ a události “Výpočet mzdy“.

2.1 Ochrana osobních dat

Zaměstnavatel přichází do styku s velkým množstvím údajů o zaměstnancích považovaných za osobní data. Tato osobní data podléhají zákonu č. 101/2000Sb., o ochraně osobních dat. Za osobní data jsou považovány jakékoliv informace určité osoby, jejíž identitu lze přímo či nepřímo zjistit na základě evidovaného čísla, kódu a podobně. Shromažďovat a zpracovávat osobní data je povolené pouze ke stanovenému účelu a pouze po nezbytnou dobu pro daný účel. Např. pro trvání pracovněprávního vztahu.

V zásadě zaměstnavatel může zpracovávat osobní data zaměstnanců pouze s jejím souhlasem. Z tohoto pravidla je řada výjimek, kdy zaměstnavatel může bez souhlasu zaměstnance shromaždovat a uchovávat osobní data zaměstnance. Kromě osobních dat jsou dále definována citlivá data. Za citlivá data jsou považovány údaje o národnosti, etnickém nebo rasovém původu, politických postojích, náboženství, záznamy o trestném činu, filozofické přesvědčení, zdravotní stav, biometrické údaje či genetické údaje. Tato citlivá osobní data může zaměstnavatel shromaždovat a uchovávat pouze se souhlasem zaměstnance. I v tomto případě mohou nastat zvláštní výjimky a zaměstnavatel může bez souhlasu uchovávat některá data. Tyto výjimky jsou definované v zákoně. Za citlivý údaj není považována mzda zaměstnance [4].

Používání rodného čísla

Od 1.4.2004 vyšel v účinnost zákon č. 53/2004 Sb. Tento zákon přinesl změny v používání rodného čísla a nahrazuje zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech. Rodné číslo nelze používat (kromě účelu statní správy a soudu) bez nositele rodného čísla nebo zákonného zástupce. V ZP není nikde definována nutnost používání rodného čísla na pracovněprávních listinách. Zaměstnavatel rodná čísla musí evidovat pro daňové účely a pro odvod na sociálním a zdravotním pojištění [4].

2.2 Historie odměňování práce

Na našem území se poprvé právní zákony ohledně odměňování práce vyskytly v horním zákoníku (*Ius regale montanorum* nebo známý také pod *Constitutiones iuris metallici*) Václava II v roce 1300. Zákoník stanovil podmínky pro těžbu a zpracování stříbra, zavedení mince Pražský groš, ale taky obsahoval pravidla pro zajištění bezpečnosti práce, pravidla pro výplatu mezd, pracovní dobu a zakazoval horníkům a kovářům samostatně se organizovat ve spolcích. Pracovní doba byla pětidenní a mzda byla vyplacená v sobotu. Zákoník byl vytvořen pomoci právníků z Itálie. Tento zákoník tohoto druhu byl první, a proto byl přeložen a používán v mnoha zemích světa. V roce 1834 byl nahrazen obecným horním zákoníkem.

Pracovní smlouva mohla být jedna ze třech typů. Smlouva čelední se uzavírala na dobu určitou a to jeden rok. Odměna za práci byla vyplacena až po skončení stanoveného období. Během pracovního období měl čeledník pouze nárok na ubytování a stravu. Další dva typy smluv byly upraveny cechovním právem a to učednická a tovaryšská. Tyto dvě smlouvy spadaly do městského práva.

V roce 1859 byl vydán živnostenský řád, který umožňoval svobodné podnikání, a pro rozvoj kapitalismu byly odstraňovány cechy. Tento zákon měl důležitou novelizaci roku 1885 a obsahoval různé sociální prvky. Také stanovoval ochranu při výplatě mzdy.

V roce 1918 byl vydán zákon o stanovení osmihodinové pracovní doby. Rovněž byl stanoven pojem práce přesčas. Zákon dále stanovil, jak bude práce přesčas proplácena. O rok později byl přijat zákon, kde byla stanovena minimální mzda pro některé velmi málo placené profese. Česká republika byla první zemí z evropských států, kde se minimální mzda začala používat. V tomto roce se zaváděly mzdové úřady, které měly řešit mzdové spory.

Později došlo k právní úpravě, která zajišťovala náhradu mzdy o státních svátcích. Také z práce v těchto dnech byl v roce 1946 zaveden stoprocentní příplatek.

V roce 1965 bylo ucelené pracovní právo a byl vyhlášen zákon č. 65/1965 Sb. zákoník práce. Zákoník práce upravuje diskriminaci v pracovně právních vztazích. Dále náhradu škody, speciální pracovní podmínky např. pro těhotně ženy, skončení pracovního poměru, pracovní doba, dovolená, překážka v práci, bezpečnost v práci, atd. Práce byla často odměňována podle množství a kvality. Mzdové tarify nařizovaly minimální, ale i maximální mzdu.

V roce 1989 po politických změnách muselo dojít k úpravám v pracovně právních vztazích. Ekonomické reformy a mzdová reforma jsou zaznamenány v usnesení vlády č. 887/1990. V roce 2007 nabyl účinnosti zákoník práce č. 262/2006 Sb., který zrušil dřívější zákoník práce č. 65/1965 Sb.

2.3 Zaměstnanec, zaměstnavatel

Zaměstnanec – jedná se o fyzickou osobu je účastníkem pracovně právního vztahu.

Zaměstnavatel – jedná se právnickou osobu jako např. obchodní společnost nebo se může jednat o fyzickou osobu jako např. živnostník. Zaměstnavatelem je i stát.

2.4 Mzda, minimální mzda

Mzda je definována v zákoníku práce dle §113 ZP[4] až §121 ZP v hlavě II. Platem se zákoník práce zabírá v §122 ZP až §137 ZP. Základní rozdíl mezi mzdou a platem je, že mzda náleží zaměstnanci v soukromém sektoru a plat v rozpočtovém (státní, nepodnikatelský) sektoru za vykonanou práci.

Mzda musí být sjednána v kolektivní, pracovní, nebo jiné smlouvě před zahájením výkonů práce, za kterou bude zaměstnanci mzda vyplacena (§113 ZP). Zaměstnavatel musí respektovat nařízení vlády o minimální mzdě (§111 ZP), kterou stanoví. Zaměstnavatel může v kolektivní smlouvě upravit výši minimální mzdy a to jedině navýšením. Podle §111ZP se minimální mzda stanovuje k počátku kalendářního roku s přihlédnutím k vývoji mezd a spotřebitelských cen. Zaměstnavatel je povinen poskytnout doplatek pokud mzda, plat nebo odměna nedosáhne minimální mzdy.

Za práci stejnou nebo srovnatelně složitou musí zaměstnavatel poskytnout stejný plat. Zaměstnavatel nesmí zvýhodňovat určitou skupinu lidí.

Dle nařízení vlády NV[5] 567/2006 Sb. §2 je minimální mzda pro týdenní pracovní dobu 40hodin stanovena na 48,10Kč na hodinu nebo 8000Kč za měsíc.

Pro invalidní osoby, mladistvé a osoby ve věku od 18 do 21let lze poskytnout mzdu v nižší částce než je minimální mzda dle nařízení vlády NV 567/2006 Sb. §4.

- 90% z minimální mzdy pro první pracovní poměr po dobu prvních šesti měsíců pro zaměstnance ve věku 18 až 21 let
- 80% z minimální mzdy pro mladistvé zaměstnance
- 75% z minimální mzdy pro zaměstnance částečného invalidního důchodu
- 50% z minimální mzdy pro zaměstnance plného invalidního důchodu a pro mladistvého zaměstnance, který je plně invalidní

[4] ZP – zákoník práce

[5] NV – nařízení vlády

Stupnice platových tarifů podle platových tříd a platových stupňů (v Kč) dle § 5 odst. 3 nařízení vlády č. 564/2006 Sb.

Plátový stupeň	**Počet let praxe**	**Plátová třída**							
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	do 1	7160	7770	8430	9140	9920	10750	11660	12660
2	do 2	7430	8070	8750	9490	10300	11160	12100	13140
3	do 4	7710	8380	9080	9850	10690	11580	12560	13640
4	do 6	8000	8700	9430	10220	11100	12020	13040	14160
5	do 9	8310	9030	9790	10610	11520	12480	13530	14700
6	do 12	8630	9370	10160	11010	11960	12950	14040	15260
7	do 15	8960	9730	10550	11430	12410	13440	14570	15840
8	do 19	9300	10100	10950	11860	12880	13950	15120	16440
9	do 23	9650	10480	11370	12310	13370	14480	15690	17060
10	do 27	10020	10880	11800	12780	13880	15030	16280	17710
11	do 32	10400	11290	12250	13260	14410	15600	16900	18380
12	nad 32	10800	11720	12710	13760	14960	16190	17540	19080

Tabulka 1: Platové třídy

Plátový stupeň	**Počet let praxe**	**Plátová třída**							
		9	**10**	**11**	**12**	**13**	**14**	**15**	**16**
1	do 1	13730	14890	16180	17530	19010	20630	22390	24290
2	do 2	14250	15450	16790	18190	10730	21410	23240	25210
3	do 4	14790	16040	17430	18880	20480	22220	24120	26160
4	do 6	15350	16650	18090	19590	21250	23060	25030	27150
5	do 9	15930	17280	18770	20330	22050	23930	25970	28170
6	do 12	16530	17930	19480	21100	22880	24830	26950	29230
7	do 15	17160	18610	20220	21900	23740	25770	27970	30330
8	do 19	17810	19310	20980	22730	24640	26740	29030	31470
9	do 23	18480	20040	21770	23590	25570	27750	30130	32660
10	do 27	19180	20800	22590	24480	26540	28800	31270	33890
11	do 32	19910	21590	23440	25400	27540	29890	32450	35170
12	nad 32	20660	22410	24330	26360	28580	31020	33670	36500

Tabulka 2: Platové třídy

Platové třídy dle §4 nařízení vlády 469/2002 Sb.:

- 1. a 2. platová třída – základní vzdělání
- 3. a 4. platová třída – střední odborné vzdělání

- 5. – 8. platová třída – úplné střední vzdělání
- 9. platová třída – vyšší odborné vzdělání
- 10. platová třída – vysokoškolské vzdělání – bakalářské
- 11. – 15. platová třída – vysokoškolské vzdělání – magisterské
- 16. platová třída – vysokoškolské vzdělání – magisterské nebo doktorské

Příklad:

Stanovte minimální mzdu pro mladistvého zaměstnance. Maximální týdenní pracovní doba u mladistvého pracovníka je 30hod.:

40 hod. týdenní doba (Kč/měsíc): $40HTPD = 80\% \cdot MM = 0{,}8 \cdot 8000 = 6800$ [6]

30 hod. týdenní doba (Kč/měsíc): $30HTPD = \frac{80\% \cdot MM}{40} \cdot 30 = \frac{0{,}8 \cdot 8000}{40} \cdot 30 = 4800$ [7]

2.5 Příplatky a odměny

Zaměstnavatel musí poskytnout příplatky a odměny:

- Za práci přesčas
- Za práci ve svátek
- Za práci ve ztíženém a zdraví škodlivém prostředí
- Za práci v noci
- Odměna za pracovní pohotovost

Mzda nebo náhradní volno za práci přesčas

Pokud vznikne právo zaměstnanci na mzdu za práci přesčas, zaměstnavatel je povinen poskytnout příplatek ve výši nejméně 25% průměrného měsíčního výdělku (§114 ZP). Při práci přesčas v období trvalého odpočinku v týdnu je příplatek minimálně 50% průměrného hodinového výdělku. Místo příplatku se může zaměstnavatel se zaměstnancem dohodnout na náhradním volnu za práci vykonanou přesčas. Pokud si zaměstnanec nevybere náhradní volno za práci přesčas do tří měsíců, případně podle dohody, náleží zaměstnanci stanovený příplatek.

[6] 40HTPD – 40hod. týdenní pracovní doba, MM – minimální mzda

[7] 30HTPD – 30hod. týdenní pracovní doba

Práce přesčas je konána na příkaz zaměstnavatele nebo se souhlasem zaměstnavatele nad stanovenou pracovní dobu (§93 ZP a §98 ZP). Zaměstnavatel může nařídit práci přesčas maximálně 8hodin za týden. Za rok nesmí doba překročit 150hodin. Roční limit se snižuje o poskytnutí náhradního volna.

Roční limit lze zvětšit na 417 hodin za rok, ale pouze se souhlasem zaměstnance. Pokud zaměstnanec pracuje jen část roku, celkový roční limit se zmenšuje v daném poměru.

Státní zaměstnanci a rozpočtové organizace se řídí jiným zákonem o práci přesčas a to č.143/1992Sb. §10. Za práci přesčas zaměstnanci přísluší část platového tarifu, osobního a zvláštního příplatku. Ten je vypočítán na hodinu, jako by byla práce konána bez práce přesčas. Dále se připočítá příplatek 25% průměrného hodinového výdělku. Za práci přesčas může zaměstnanec využít náhradní volno a to do tří měsíců od konání práce přesčas. Pokud zaměstnanec využije čerpání náhradního volna, plat se nekrátí.

Příklad:

Zaměstnanec má základní měsíční mzdu 15000Kč. Průměrný výdělek činí 75Kč na hodinu. Zaměstnanec odpracoval 168hodin a fond pracovní doby je stanoven na 168 hodin. Dále vykonal dalších 20hodin práci přesčas. Jak se změní mzda zaměstnance včetně příplatku?

Základní mzda: 15000Kč

Mzda za přesčas (Kč): $MPP = \frac{ZM}{fond\ \ prac.doby} \cdot OPP = \frac{15000}{168} \cdot 20 =$ [8]

$1785,71 \cong 1786$

Příplatek za práci přesčas (Kč): $PPP = OPP \cdot PHV \cdot PPPP = 20 \cdot 75 \cdot 0,25 = 375$ [9]

Celková mzda (Kč): $CM = ZM + MPP + PPP = 15000 + 1786 + 375 = 17161$ [10]

Mzda, náhradní volno nebo náhrada mzdy za práci ve svátek

Pokud vznikne právo zaměstnanci na mzdu za práci ve svátek, zaměstnavatel je povinen poskytnout příplatek ve výši nejméně 100% průměrného měsíčního výdělku (§115 ZP). Místo příplatku se může zaměstnavatel se zaměstnancem dohodnout na náhradním volnu za práci vykonanou přesčas. Pokud si zaměstnanec nevybere náhradní volno za práci přesčas do tří měsíců, případně podle dohody, náleží zaměstnanci stanovený příplatek. Pokud zaměstnanec s hodinovou mzdou v době svátku, který připadá na jeho pracovní den, nepracuje, přísluší mu

[8] MPP – mzda za práci přesčas, ZM – základní mzda, OPP – odpracoval práci přesčas

[9] PPP – příplatek za práci přesčas, PHV – průměrný hodinový výdělek, PPPP – procentní příplatek za práci přesčas

[10] CM – celková mzda

náhrada mzdy. Náhrada mzdy je ve výši průměrného výdělku nebo pouze část mzdy, kterou je ve ztrátě důsledkem svátku (§115 ods.3 ZP).

Pokud zaměstnanec dostává měsíční mzdu a v den svátku nepracuje, pak mu je vyplacena stále stejná mzda za předpokladu, že odpracoval řádně celý měsíc.

Příklad:

Zaměstnanec má základní hodinovou mzdu 75Kč. Průměrný výdělek činí 85Kč na hodinu. Zaměstnanec odpracoval 170hodin a fond pracovní doby je stanoven na 160 hodin. Tedy odpracoval 10hodin ve svátek. Zaměstnanec má 8hod. pracovní dobu. Jaká bude mzda zaměstnance včetně příplatku?

Základní mzda (Kč): $ZM = OC \cdot ZHV = 160 \cdot 75 = 12000$ [11]

Mzda za svátek (Kč): $MS = OS \cdot ZHV = 10 \cdot 75 = 750$ [12]

Příplatek za práci ve svátek (Kč): $PPS = OS \cdot PHV \cdot PPPS = 10 \cdot 85 \cdot 1 = 850$ [13]

Celková mzda (Kč): $CM = ZM + MS + PPS = 12000 + 750 + 850 = 13600$

Příklad:

Zaměstnanec má základní měsíční mzdu 15000Kč. Průměrný výdělek činí 85Kč na hodinu. Zaměstnanec nepracoval o svátku, na který připadá 8hodin v pracovní den. Fond pracovní doby je 168hodin. Jak se změní mzda zaměstnance včetně příplatku?

Základní mzda (Kč): $ZM = 15000$

Příplatek za práci ve svátek (Kč): $PPS = OS \cdot PHV \cdot PPPS = 0 \cdot 85 \cdot 1 = 0$

Celková mzda (Kč): $CM = ZM + PPS = 15000 + 0 = 15000$

Mzda a příplatek za noční práci

Pokud vznikne právo zaměstnanci na mzdu a příplatek za noční práci (§116 ZP), zaměstnavatel je povinen poskytnout příplatek ve výši nejméně 10% průměrného výdělku. V kolektivní smlouvě může být stanovena jiná výše příplatku. Noční směna je od 22:00hodin do 6:00hodin. Noční směna se počítá do dne, kdy začala.

[11] OC – odpracovaná doba celkem, ZHV – základní hodinový výdělek

[12] MS – mzda za svátek, OS – odpracována doba ve svátek

[13] PPS – příplatek za práci přesčas, PPPS – procentní příplatek za práci ve svátek

Příklad:

Zaměstnanec má základní měsíční mzdu 15000Kč. Fond pracovní doby je 168hodin. Zaměstnanec z toho odpracoval 40hodin v noci a zbytek ve dne. Průměrný měsíční výdělek činí 80Kč na hodinu. Jak se změní mzda zaměstnance včetně příplatku?

Základní mzda (Kč): $ZM = 15000$

Příplatek za práci v noci (Kč): $PPV = OV \cdot PHV \cdot PPPV = 40 \cdot 80 \cdot 0{,}1 = 320$ [14]

Celková mzda (Kč): $CM = ZM + PPV = 15000 + 320 = 15320$

Mzda a příplatek za práci ve ztíženém pracovním prostředí

Pokud vznikne právo zaměstnanci na mzdu a příplatek za práci ve ztíženém pracovním prostředí (§117 ZP), zaměstnavatel je povinen poskytnout příplatek ve výši nejméně 10% dle zákona §111 ZP ods.2 ZP o minimální mzdě. Tedy minimálně 10% ze základu minimální mzdy zaměstnance. Vymezení stižených pracovních podmínek stanoví nařízení vlády pro účely odměňování. Za ztížené pracovní prostředí lze např. považovat: prach, chemické látky, ustálený nebo proměnný hluk, impulzní hluk, vibrace přenášené na ruce, zvýšený tlak nad 400kPa, atd.

Příklad:

Zaměstnanec má základní měsíční mzdu 15000Kč. Zaměstnanec odpracoval celý měsíc ve ztíženém pracovním prostředí. Jak se změní mzda zaměstnance včetně příplatku?

Základní mzda (Kč): $ZM = 15000$

Příplatek za ztížené pracovní prostředí (Kč): $PPZ = OZ \cdot PHV \cdot PPPZ = 15000 \cdot 0{,}1 = 1500$ [15]

Celková mzda (Kč): $CM = ZM + PPZ = 15000 + 1500 = 16500$

Mzda a příplatek za práci v sobotu a neděli

Pokud vznikne právo zaměstnanci na mzdu a příplatek za práci v sobotu a neděli (§118 ZP), zaměstnavatel je povinen poskytnout příplatek ve výši nejméně 10% průměrného výdělku.

[14] PPV – příplatek za práci v noci, OV – odpracována doba v noci, PPPV – procentní příplatek za práci v noci

[15] PPZ – příplatek za práci ve stiženém pracovním prostředí, OZ - odpracována doba ve stiženém pracovním prostředí, PPPZ – procentní příplatek za práci ve stiženém pracovním prostředí

Příklad:

Zaměstnanec má základní měsíční mzdu 15000Kč. Fond pracovní doby je 168hodin. Zaměstnanec odpracoval navíc 8hodin o víkendu. Průměrný měsíční výdělek činí 90Kč na hodinu. Jak se změní mzda zaměstnance včetně příplatku?

Základní mzda (Kč): $ZM = 15000$

Mzda za práci v sobotu a neděli (Kč): $MN = \frac{ZM}{fondprac.doby} \cdot ON = \frac{1500}{168} \cdot 8 = 715$ [16]

Příp. za práci v sobotu a neděli (Kč): $PPN = ON \cdot PHV \cdot PPPN = 8 \cdot 90 \cdot 0{,}1 = 72$ [17]

Celková mzda (Kč): $CM = ZM + MN + PPN = 15000 + 715 + 72 = 15787$

Odměna za pracovní pohotovost

Pokud vznikne právo zaměstnanci na mzdu odměna za pracovní pohotovost (§140 ZP), zaměstnavatel je povinen poskytnout odměnu ve výši nejméně 10% průměrného výdělku. V kolektivní smlouvě může být stanovena jiná výše odměny. Pokud má zaměstnanec nařízenou pracovní pohotovost, nenáleží mu za to mzda. Zaměstnanec má nárok pouze na odměnu za pohotovost. Jestliže zaměstnanec má nařízenou pohotovost na pracovišti odměna za pohotovost je 50% průměrného výdělku. Pokud zaměstnanec v době pracovní pohotovosti pracuje, je tato práce považována za práci přesčas pokud překročí týdenní pracovní dobu. Pokud je pohotovost v rámci práce přesčas, je potřeba hlídat limity pro práci přesčas.

Příklad:

Zaměstnanec má průměrný výdělek 60Kč na hodiny. Zaměstnanec měl nařízenou domácí pohotovost v rozsahu 20hodin. Během této doby nemusel jít do práce. Jaká bude odměna za pracovní pohotovost?

Celková odměna (Kč): $CO = PHV \cdot PPPPD \cdot OPD = 60 \cdot 0{,}1 \cdot 20 = 120$ [18]

2.6 Průměrný výdělek

Průměrný výdělek je definován v zákoníku práce pod §351 ZP až §362 ZP v hlavě XVIII. Průměrný výdělek zaměstnance se zjišťuje z hrubé mzdy (platu) zaúčtované k výplatě a

[16] MN – mzda za práci v sobotu a neděli, ON odpracována doba v sobotu a neděli

[17] PPN – příplatek za práci v sobotu a neděli, PPPN – procentní příplatek za práci v sobotu a neděli

[18] CO – celková odměna, PPPPD – procentní příplatek za pohotovost strávenou doma, OPD – doba domácí pohotovosti

z odpracované doby v rozhodném období (§353 ZP). Odpracovaná doba je doba, za kterou náleží zaměstnanci mzda. Za rozhodné období je považováno předchozí kalendářní čtvrtletí, pokud není stanoveno jinak (§354 ZP). Do základu pro výpočet průměrného výdělku se počítají částky, které souvisí přímo s odpracovanou dobou. Nelze do základu započítat např. náhradu mzdy za nemoc nebo náhradu mzdy za neodpracovaný svátek v pracovní den. Podle zaměstnavatele může být průměrný výdělek stanoven na den nebo hodinu a to tak, že se suma částek vydělí odpracovanou dobou v hodinách nebo dnech.

Podle §355 ZP lze použít pravděpodobnostní výdělek a to v případech kdy zaměstnanec v rozhodném období neodpracoval alespoň 21dní. Tato situace může nastat novým nástupem do zaměstnání, dlouhotrvající nemoci a podobně. Pravděpodobnostní výdělek se počítá z hodnot, které zaměstnanec dosáhl od počátku rozhodného období nebo z předpokládaného hrubého výdělku, kterého by v daném období dosáhl.

Přepočet z průměrného hodinového výdělku na průměrný měsíční výdělek je podle §356 ZP následovný: Průměrný rok má 365,25dnů. Průměrný hodinový výdělek se vynásobí týdenní pracovní dobou zaměstnance a koeficientem 4,348, což je průměrný počet týdnů na jeden měsíc.

Příklad:

Zaměstnanec má základní měsíční mzdu 10000Kč. Zaměstnanec odpracoval za čtvrtletí 480hodin + 20hodin přesčas v pracovní dny a vyčerpal 40hodin dovolené. Dále dostal každý měsíc prémie 1000Kč a osobní ohodnocení ve třetím měsíci 3500Kč. Průměrný hod. výdělek činil 65Kč na hodinu. V prvním měsíci dostal 10000Kč. Ve druhém měsíci měl dovolenou 40hodin, tedy dostal 10328Kč a z toho náhrada mzdy činila 2600Kč. Ve třetím měsíci zaměstnanec odpracoval 20hodin přesčas (fond pracovní doby byl 176hodin). Zaměstnanec vydělal 11462Kč, z toho 1137Kč je náhrada mzdy za přesčas a 325Kč příplatek za přesčas. Jaký bude průměrný výdělek na další čtvrtletí?

Celková mzda za 1. měsíc (Kč): $CM1 = ZM + P = 10000 + 1000 = 11000$ [19]

Celková mzda za 2. měsíc (Kč): $CM2 = (ZM - NMD) + P = (10328 - 2600) + 1000 = 8728$ [20]

Celková mzda za 1. měsíc (Kč): $CM3 = (ZM + MPP + PPP) + P + OO = (10000 + 1137 + 325) + 1000 + 3500 = 15962$ [21]

Celková mzda (Kč): $3CM = CM1 + CM2 + CM3 = 11000 + 8728 + 15962 = 35690$ [22]

[19] CM1 – celková mzda za první měsíc, P - prémie

[20] CM2 – celková mzda za druhý měsíc, NMD – náhrada mzdy za dovolenou

[21] CM3 – celková mzda za třetí měsíc, OO – osobní ohodnocení

Odpracovaná doba celkem (hodin): $3OC = OC + OPP = 480 + 20 = 500$ [23]

Průměrný hodinový výdělek (Kč): $PHV = \frac{3CM}{3OC} = \frac{35690}{500} = 71{,}38$

2.7 Dovolená

Dovolená je definována v zákoníku práce pod §211 ZP až §223 ZP. Dle §211 ZP zaměstnanec má nárok na dovolenou za kalendářní rok, nebo pokud je zaměstnanec kratší dobu zaměstnán, tak má nárok na její poměrnou část. Dále to může být dovolená za odpracované dny nebo dodatková dovolená. Dovolená přísluší zaměstnanci až po vykonání 60 kalendářních dnů nepřetržitého pracovního poměru. Dovolená podle §213 odst. 1 ZP činí nejméně 4týdny v kalendářním roce. Dovolená některých zaměstnanců se může lišit. Jsou to např. zaměstnanci uvedení v §109 odst. 3 ZP, kteří mají nárok na 5týdnů dovolené. Dále to jsou skupiny pedagogických a akademických pracovníků, kteří mají nárok na 8 týdnů dovolené v kalendářním roce.

Pokud dovolená trvá necelý den, zaokrouhluje se na půlden (§216 ZP). Připadne-li na den zahrnutí v dovolené státní svátek, pak se tento den nepočítá do dovolené. Taky se nesmí překrývat náhradní volno s dovolenou.

Jestliže zaměstnanec čerpá dovolenou, je zaměstnavatel povinen za tuto dobu poskytnout zaměstnanci náhradu mzdy (§222 ZP). Náhrada mzdy za dovolenou je ve výši průměrného výdělku. Zaměstnanci může náležet také náhrada za 4 týdny nevyčerpané dovolené. Na tuto náhradu má zaměstnanec nárok, pokud nemohl vyčerpat dovolenou do příštího kalendářního roku nebo pokud se zaměstnavatelem ukončil pracovní poměr.

Zaměstnavatel má možnost zaměstnanci krátit dovolenou (§223 ZP). Například za neomluvenou zameškanou směnu může zaměstnavatel zaměstnanci zkrátit dovolenou o 1 až 3 dny. Zaměstnanci, kterému je krácená dovolená, musí být poskytnuta dovolena za kalendářní rok nejméně v délce 2 týdnu.

Příklad:

Zaměstnanec si vybere 5 dnů dovolené. Jeho průměrný hod. výdělek činil 65Kč na hodinu. Zaměstnanec má 8 hodinovou pravidelnou pracovní dobu. Jaká bude náhrada mzdy za dovolenou?

Náhrada mzdy (Kč): $NMD = PHV \cdot PD \cdot DD = 65 \cdot 8 \cdot 5 = 2600$ [24]

---

[22] 3CM – celková mzda za tři měsíce

[23] 3OC – celková odpracována doba za tři měsíce

[24] PD – pracovní doba, DD – počet dnů dovolené

2.8 Náhrada mzdy při pracovní neschopnosti

Od 1. 1. 2009 vstoupil platnost zákon č. 187/2006 Sb. Tento zákon se zabývá nemocenským pojištěním. Tento zákon stanovuje, že nemocenská se počítá zaměstnancům vždy až od 15. kalendářního dne trvání nemocí nebo karantény. Za prvních 14 dní je povinen podle zákona zabezpečit zaměstnance zaměstnavatel. Zaměstnavatel poskytuje náhradu mzdy podle §192 - §194 ZP, zákon č. 585/2006 Sb., zákon č. 261/2007 Sb., zákon č. 305/2008Sb.

Zaměstnavatel je povinen poskytnout náhradu mzdy zaměstnanci v pracovním poměru nebo zaměstnancům s dohodou o pracovní činnosti. Náhrada mzdy přísluší pouze za pracovní dny případně za svátky, za které zaměstnanci přísluší náhrada mzdy.

Zaměstnanec má nárok na náhradu mzdy ve dvou případech:

- Při dočasné pracovní neschopnosti
- Při karanténě

Při dočasné pracovní neschopnosti zaměstnanci nenaleží náhrada mzdy za první tři dny. Náhrada mzdy přísluší zaměstnanci ve výši 60% PRHV[25] od 4. pracovního dne.

Při karanténě náhrada mzdy přísluší zaměstnanci ve výši 25% PRHV během prvních třech dnů. Dále ve výši 60% PRHV od 4. pracovního dne.

Období prvních 14 kalendářních dnů se počítá od data vzniku pracovní neschopnosti, nebo pokud je směna ukončena, tak od následujícího dne. Pokud v den začátku pracovní neschopnosti zaměstnanec čerpá dovolenou nebo je tento den svátek, počítá se začátek pracovní neschopnosti od tohoto dne. Začátek pracovní neschopnosti může začít dnem, kdy zaměstnanec neodpracuje celou směnu z důvodu pracovní neschopnosti. Období 14 kalendářních dnů končí uplynutím 14. kalendářního dne ve 24:00hodin (např. pokud zaměstnanci na tento den připadá noční).

Pro výpočet náhrady mzdy při DPN[26] je potřeba stanovit PHV[27] viz kapitola 2.5 Průměrný výdělek. PHV se zjišťuje za předchozí čtvrtletí. Pokud nemoc do 14. kalendářního dne bude trvat přes toto čtvrtletí, je nutné pro výpočet náhrady mzdy použít tyto dva PHV.

PHV se dále pro náhradu mzdy při DPN musí upravit na RPHV. Tato úprava probíhá stejně jako úprava denního vyměřovacího základu pro výpočet nemocenské. Jsou stanovené tří redukční hranice a pro rok 2009 následovně:

- I. *786Kč*
- II. *1178Kč*
- III. *2356Kč*

[25] PRHV - průměrný redukovaný výdělek
[26] DPN - Dlouhodobá pracovní neschopnost
[27] PHV – průměrný hodinový výdělek

Tyto redukční hranice pro daný rok se vyhlašují ve sbírce zákonů sdělením Ministerstva práce a sociálních věcí. Pro stanovení RPHV se musí tyto denní redukční hranice přepočítat na hodinové redukční hranice. Pro přepočet se používá koeficient 0,175. Výsledek se zaokrouhluje na haléře směrem nahoru. Hodinové redukční hranice jsou:

- I.HRH[28] $786 \cdot 0,175 = 137,55Kč$
- II.HRH[29] $1178 \cdot 0,175 = 206,15Kč$
- III.HRH[30] $2356 \cdot 0,175 = 412,30Kč$

Následně je potřeba provést pomocí hodinových redukčních hranic redukci PHV následovně:

- Do výše první redukční hranice 90%
- Rozdíl mezi druhou a první redukční hranici 60%
- Rozdíl mezi třetí a druhou redukční hranici 30%
- Částka PHV nad třetí redukční hranici se nezapočítává

RPHV se následně stanoví jako součet těchto upravených hodinových redukčních hranic (redukce PHV). Následně se z RPHV vypočítává hodinová náhrada mzdy. Pro karanténu v prvních třech dnech činí 25% z RPHV. Od 4 do 14 dne činí 60% z RPHV.

Pro výpočet celkové náhrady mzdy se hodinová náhrada mzdy vynásobí počtem neodpracovaných hodin zaměstnance za prvních 14kalendářních dnů trvání pracovní neschopnosti. Výsledná náhrada mzdy se zaokrouhluje směrem nahoru (§142 ZP).

Příklad:

Stanovte maximální redukovaný průměrný výdělek. Stanovte také maximální náhrady mzdy při karanténě a pracovní neschopnosti.

Maximální redukovaný průměrný výdělek:

I.HRPV[31] (Kč): $I.HRPV = I.HRH \cdot 90\% = 137,55 \cdot 0,9 = 123,795$

II.HRPV[32] (Kč): $II.HRPV = (II.HRH - I.HRH) \cdot 60\% = (206,15 - 137,55) \cdot 0,6 = 41,16$

III.HRPV[33] (Kč): $III.HRPV = (III.HRH - II.HRH) \cdot 30\% = (411,30 - 206,15) \cdot 0,3 = 61,845$

[28] I.HRH – první hodinová redukční hranice
[29] II.HRH – druhá hodinová redukční hranice
[30] III.HRH – třetí hodinová redukční hranice
[31] I.HRPV – první hranice hodinového redukovaného průměrného výdělku
[32] II.HRPV – druhá hranice hodinového redukovaného průměrného výdělku

Maximální redukovaný průměrný výdělek je (Kč):

$$MRPV = I.HRH + II.HRH + III.HRH = 123,795 + 41,16 + 61,845 = 226,80$$ [34]

Maximální denní náhrada mzdy pří karanténě (první tři dny v Kč):

$$MNMK = MRPV \cdot 25\% = 226,80 \cdot 0,25 = 56,70$$ [35]

Maximální denní náhrada mzdy při pracovní neschopnosti nebo karanténě (3. až 14. den v Kč):

$$MNMN = MRPV \cdot 60\% = 226,80 \cdot 0,6 = 136,08$$ [36]

Příklad:

Zaměstnanec má 40hodinovou týdenní pracovní dobu. Denní pracovní doba je 8hodin. Průměrný hodinový výdělek je 245,25Kč. DPN trvala 14dní a zaměstnanec neodpracoval 10směn. Stanovte náhradu mzdy?

Redukovaný průměrný výdělek:

Částka PHV do 137,55Kč se započítá ve výši 90% (Kč):

$$I.HRPV = I.HRH \cdot 90\% = 137,55 \cdot 0,9 = 123,795$$

Rozdíl mezi II. a I. redukční hranici ve výši 60% (Kč):

$$II.HRPV = (II.HRH - I.HRH) \cdot 60\% = (206,15 - 137,55) \cdot 0,6 = 41,16$$

Rozdíl mezi III. a II. redukční hranici ve výši 30% (Kč):

$$III.HRPV = (III.HRH - II.HRH) \cdot 30\% = (245,25 - 206,15) \cdot 0,3 = 11,73$$

Redukovaný průměrný hodinový výdělek činí (Kč):

$$RPHV = I.HRH + II.HRH + III.HRH = 123,795 + 41,16 + 11,73 = 176,685$$ [37]

Denní hodinová náhrada mzdy při pracovní neschopnosti (Kč):

$$HNMN = RPHV \cdot 60\% = 176,685 \cdot 0,6 = 106,011$$ [38]

Za první tři dny náhrada mzdy nenáleží. Náhrada mzdy za další dny (Kč):

$$NMN = ND \cdot PD \cdot HNMN = (10 - 3) \cdot 8 \cdot 106,011 = 5936,616 \cong 5937$$ [39]

---

[33] III.HRPV – třetí hranice hodinového redukovaného průměrného výdělku

[34] MRPV – maximální redukovaný průměrný hodinový výdělek

[35] MNMK – maximální náhrada mzdy při pracovní neschopnosti - karanténa

[36] MNMN - maximální náhrada mzdy při pracovní neschopnosti - nemoc

[37] RPHV – redukovaný průměrný hodinový výdělek

[38] HNMN – denní hodinová náhrada mzdy při pracovní neschopnosti

2.9 Naturální mzda

Naturální mzda (§119 ZP) je forma mzdy, která není poskytována ve finančních prostředcích. Zákon umožňuje poskytovat část mzdy ve formě naturální mzdy. Tuto naturální mzdu může zaměstnavatel poskytnout pouze se souhlasem zaměstnavatele a po vzájemně dohodnutých podmínkách. V rámci naturální mzdy můžou být poskytnuté výrobky (kromě lihovin, tabákových výrobků a jiných návykových látek). Dále za naturální mzdu se může považovat poskytnutí výkonů, práce a služeb.

Výše naturální mzdy musí odpovídat ceně, kterou zaměstnanec účtuje za stejné výrobky případně služby či práci nebo musí odpovídat rozdílu, o který jsou výrobky, služby či práce nižší. Minimální mzdu nelze poskytovat v naturální mzdě. Minimální mzdu musí zaměstnavatel vždy vyplatit v penězích. Plat na rozdíl od mzdy nelze vyplácet v naturální formě.

2.10 Sociální pojištění

Sociálním pojištěním se přispívá na úhradu těchto složek:

- Dávky důchodového pojištění (důchody starobní, plný invalidní, částečný invalidní, sirotčí, vdovský a vdovecký)
- Dávky nemocenského pojištění (nemocenská, podpora při ošetřování, příspěvek v mateřství, peněžitá pomoc v mateřství, příspěvek v těhotenství)
- Podpora nezaměstnanosti, na správní výdaje ČSSZ[40] a úřady práce

Každý zaměstnanec je povinný platit tyto složky sociálního pojištění. Zaměstnanec platí důchodové pojištění, další dvě platí zaměstnavatel. U osob OSVČ[41] platí jiná pravidla. Osoba OSVČ může dobrovolně platit nemocenské pojištění. Ostatní dvě složky jsou pro osoby OSVČ povinné. Období pro stanovení vyměřovacího základu pro zaměstnance je stanovené na jeden kalendářní měsíc.

Od 1. 1. 2008 je zaveden strop pro odvod na sociálním pojištění. Tento strop je na celý kalendářní rok stanoven jako 48 násobek průměrné mzdy.

Dle zákona č. 589/1992 Sb. §7 jsou sazby z vyměřovacího základu následující:

- U zaměstnanců 6,5% z hrubé mzdy
- OSVČ 29,2% a dobrovolné nemocenské pojištění 1,4%

[39] NMN – náhrada mzdy za pracovní neschopnost, ND – počet dní pracovní neschopnosti pro náhradu mzdy

[40] ČSSZ – česká správa sociálního zabezpečení

[41] OSVČ – osoby výdělečné činné

- U zahraničních zaměstnanců 2,4%
- Dobrovolně účastné osoby důchodového pojištění 28%
- Organizace a malé organizace 25%

U organizací jsou odvody na sociální pojištění stanovené na 25%. Z těchto 25% připadá na nemocenské pojištění 2,3%, na důchodové pojištění 21,5% a na politiku zaměstnanosti se přispívá 1,2%.

U OSVČ jsou odvody na sociální pojištění stanovené na 28% na důchodové pojištění, 1,2% na politiku zaměstnanosti a dobrovolné nemocenské pojištění 1,4%.

Příklad:

Zaměstnanec má v hlavním poměru zdanitelný příjem 15000Kč. Jaké budou příspěvky na sociální pojištění?

Zaměstnanec (Kč): $CPZ = ZP \cdot 6{,}5\% = 15000 \cdot 0{,}065 = 975$ [42]

Zaměstnavatel (Kč): $CPF = ZP \cdot 25\% = 15000 \cdot 0{,}25 = 3750$ [43]

2.11 Zdravotní pojištění

Zdravotní pojištění je zákonem stanovené pojištění, které slouží pro úhradu nákladů souvisejících se zdravotní péči. Nemocenská není placená ze zdravotního pojištění, ale ze sociálního pojištění. Zdravotní pojištění, až na výjimky, neplní účel úhrady zdravotních výloh v zahraničí. Dle zákona č. 48/1997 Sb. §4-§7 musí za každého pojištěnce někdo být plátcem zdravotního pojištění a dle zákonu to jsou:

- Zaměstnavatel
- Stát
- Pojištěnec (OSVČ a OBZP[44])

Zdravotní pojištění se odvádí přímo zdravotním pojišťovnám. Momentálně na území ČR působí deset těchto zdravotních pojišťoven. Každý pojištěnec má právo si vybrat jednu zdravotní pojišťovnu. Pojištěnec může zdravotní pojišťovnu změnit jednou za 12 kalendářních měsíců. Změny se provádějí k prvnímu dni kalendářního čtvrtletí. Pojištěnec je povinen nahlásit změnu zdravotní pojišťovny svému zaměstnavateli a praktickému lékaři do 8dnů.

[42] CPZ – sociální pojištění zaměstnanec, ZP – zdanitelný příjem

[43] CPF – sociální pojištění zaměstnavatel

[44] OBZP – osoba bez zdanitelného příjmu

Od platby zdravotního pojištění jsou osvobození určité skupiny lidí. Jsou to např.: nezaopatřené děti nevýdělečně činné do 26let, osoby pobírající důchod, ženy na mateřské dovolené, ženy na rodičovské dovolené, uchazeči o zaměstnání, osoby ve výkonu trestu, atd.

Osoby OBZP jsou občané s trvalým pobytem na území ČR. Za osoby není plátcem zdravotního pojištění stát a osoby neodvádí pojistné jako osoby OSVČ. Pojistné se stanovuje na základě minimální mzdy. Pro rok 2009 je minimální mzda 8000Kč a z toho je vypočítán základ na měsíční zálohy zdravotního pojištění 1080Kč.

Výše zdravotního pojištění za rozhodné období z vyměřovacího základu je stanovené dle zákona č. 592/1992 Sb. Pro zaměstnance, zaměstnavatele a OBZP je rozhodné období stanovené na 1 kalendářní měsíc. U OSVČ je rozhodné období jeden rok. Pro zaměstnance je vyměřovací základ hrubá mzda. Ze 13,5% zaměstnanec zaplatí 4,5% a zaměstnavatel zaplatí 9%. Pro OSVČ je minimální měsíční záloha na zdravotní pojištění 1590Kč.

Od roku 2008 platí maximální odvod na zdravotním pojištění. Tento strop je na kalendářní rok stanoven ve výši 48násobku průměrné mzdy. Vypočtené odvody na zdravotním pojištění se zaokrouhlují na celé koruny směrem nahoru.

Při neomluvené absenci zaměstnance v práci je zaměstnanec povinen zaplatit částku odpovídající pojistnému. Zaměstnanec je tedy povinen zaplatit celých 13,5% z minimálního vyměřovacího základu za celou dobu trvání neomluvené absence zaměstnance.

Příklad:

Zaměstnanec má v hlavním poměru zdanitelný příjem 15000Kč. Jaké budou příspěvky na zdravotní pojištění?

Zaměstnanec (Kč): $ZPZ = ZP \cdot 4{,}5\% = 15000 \cdot 0{,}045 = 675$ [45]

Zaměstnavatel (Kč): $ZPF = ZP \cdot 9\% = 15000 \cdot 0{,}09 = 1350$ [46]

2.12 Daně

Plátci daně lze rozdělit do dvou skupin. První skupina jsou tzv. rezidenti. Občané spadající do této skupiny mají na území ČR trvalý pobyt nebo jsou to občané, kteří se zde zdržují alespoň 183dnů v roce. Rezidenti musí platit daň z příjmu ze svých celosvětových příjmů. Druhá skupina jsou tzv. nerezidenti. Tyto osoby odvádějí daň ze svého příjmu, který dosáhnou pouze na území ČR. Od roku 2008 bylo pro osoby OSVČ zrušená minimální daň.

Zálohová daň se od roku 2008 platí z tzv. superhrubé mzdy. Superhrubá mzda je hrubá mzda zaměstnance zvýšená o pojistné, které platí zaměstnavatel. Tedy superhruba mzda obsahuje:

[45] ZPZ – zdravotní pojištění zaměstnanec

[46] ZPF – zdravotní pojištění zaměstnavatel

- Hrubá mzda dle pracovní smlouvy
- Příplatky, odměny
- Naturální mzda – zaměstnanecké výhody počítající se do příjmu
- Sociální a zdravotní pojištění placené zaměstnavatelem (sociální a zdravotní pojištění placené zaměstnancem se do superhrubé mzdy nezapočítávají)

Příjmy fyzických osob se v roce 2009 daní sazbou ve výši 15%. Příjmy ze zaměstnání tzv. superhrubá mzda se daní tedy 15%. Základ daně neboli superhrubá mzda se zaokrouhluje na stokoruny nahoru. Tento základ daně se zdaní a následně vznikne daň před zvýhodněním. Následně je možné uplatnit slevy na dani, na které má zaměstnanec nárok. Pro uplatňování slev na dani je potřeba, aby zaměstnanec podepsal prohlášení k dani. Součet slev na dani nemůže být větší, než je daň před zvýhodněním. Po odečtení daňových slev je možné odečíst daňové zvýhodnění (děti) a toto daňové zvýhodnění lze odečíst do minusové částky. Po odečtení slev na dani a daňového zvýhodnění dostaneme zálohovou daň. Pokud je měsíční zálohová daň minusová, jedná se o tzv. měsíční daňový bonus, který zaměstnavatel vyplatí zaměstnanci. Zaměstnanec má nárok na vyplacení daňového bonusu, pokud roční výše je alespoň 50Kč. Maximální výše měsíčního daňového bonusu je 4350Kč.

Tabulka slev na dani		
Sleva na dani	**Roční (Kč)**	**Měsíční (Kč)**
Na poplatníka	24840	2070
Částeční invalidní důchod	2540	210
Plný invalidní důchod	5040	420
Držitel průkazu ZTP/P	16140	1345
Poplatník připravující se na budoucí povolání (do 26let, u doktorského studia na VŠ[47] do 28let)	4020	335

Tabulka 3: Slevy na dani

Tabulka zvýhodnění na dítě		
Daňové zvýhodnění	**Roční (Kč)**	**Měsíční (Kč)**
Každé vyživované dítě žijící s poplatníkem v domácnosti	10680	890
Pokud dítě je držitelem ZTP/P	21360	1780

Tabulka 4: Daňové zvýhodnění

[47] VŠ – vysoká škola

Z čeho všeho se platí daň:

- Příjmy ze závislé činnosti (převážně mzda včetně naturální mzdy a plat)
- Příjmy z podnikání
- Příjmy ze samostatně výdělečné činnosti
- Příjmy z kapitálového majetku
- Příjmy z pronájmu movitých věcí, nemovitostí
- Ostatní příjmy např. výhry, prodej movitých věcí, atd.

Příklad:

Zaměstnanec má v hlavním poměru měsíční mzdu 15000Kč. Dále zaměstnanec pobírá naturální mzdu ve výši 5000Kč. Zaměstnanec doložil prohlášení k dani. Uplatňuje slevu na poplatníka a daňové zvýhodnění na tři děti. Jaká bude měsíční záloha na dani?

Hrubá mzda (Kč): $HM = 15000$ [48]

Zdanitelný příjem (Kč): $ZP = HM + NM = 15000 + 5000 = 20000$ [49]

Pojištění sociální – zaměstnanec (Kč): $CPZ = ZP \cdot 6{,}5\% = 20000 \cdot 0{,}065 = 1300$

Pojištění zdravotní – zaměstnanec (Kč): $ZPZ = ZP \cdot 4{,}5\% = 20000 \cdot 0{,}045 = 900$

Pojištění sociální – zaměstnavatel (Kč): $CPF = ZP \cdot 25\% = 20000 \cdot 0{,}25 = 5000$

Pojištění zdravotní – zaměstnavatel (Kč): $ZPF = ZP \cdot 9\% = 20000 \cdot 0{,}09 = 1800$

Základ daně (Kč): $ZD = ZP + CPF + ZPF = 20000 + 5000 + 1800 = 26800$ [50]

Daň před zvýhodněním (Kč): $DPZ = ZD \cdot 15\% = 26800 \cdot 0{,}15 = 4020$ [51]

Záloha na daň z příjmu (nemůže být záporná v Kč):

$$ZDZP = DPZ - SD - DZ = 4020 - 2070 - (3x890) = -720 = 0$$ [52]

Daňový bonus (pokud po odečtení daňového zvýhodnění je ZDZP záporná v Kč):

$$DB = DPZ - SD - DZ = 4020 - 2070 - (3x890) = -720, tedy\ bonus\ 720$$ [53]

[48] HM –hrubá mzda
[49] NM – naturální mzda
[50] ZD – základ daně
[51] DPZ – daň před zvýhodněním
[52] ZDZP – záloha na daň z příjmu, SD – sleva na dani, DZ – daňové zvýhodnění
[53] DB – daňový bonus

Čistá mzda (Kč):

$$CIM = HM - CPZ - ZPZ + DB = 15000 - 1300 - 900 + 720 = 13520$$ [54]

2.13 Srážky ze mzdy

Srážky ze mzdy jsou definované v §145 ZP a §146 ZP. Zaměstnavatel může zaměstnanci srážet peněžní prostředky na základě dohody o srážkách ze mzdy (§327 ZP) nebo jen v případě (dle §147 ZP):

- Daň z příjmu fyzických osob ze závislé činnosti
- Sociální a zdravotní pojištění
- Zálohu na mzdu nebo plat
- Nevyúčtované zálohy poskytnuté zaměstnanci (k plnění jeho pracovních úkonů)
- Náhrada mzdy nebo platu za dovolenou (pokud zaměstnanec ztratil na ní právo)
- Exekuce nařízené soudem, správcem daně, soudním exekutorem,…
- Srážky ze mzdy k náhradě škody (jen dle (§146 ZP)

Srážky se provádějí z čisté mzdy zaměstnance. Pořadí srážek určuje zákon §147 ZP a odpovídá uvedenému seznamu. Před strháváním srážek ze mzdy je potřeba vypočítat základní nezabavitelnou částku. Tato částka nesmí být podle nařízení vlády č.595/2006 Sb. zaměstnanci srážena. Částka čisté mzdy přesahující nezabavitelnou částku může být postižitelná srážkami bez omezení.

Nezabavitelné částky se stanoví podle nařízení vlády č.595/2006 Sb. a to z částek životního minima jednotlivce a částky normativních nákladů na bydlení pro jednu osobu. Částka životního minima dle zákona o životním minimu je od 1. 1. 2007 stanovena na 3126Kč. Částka normativních nákladů na bydlení je od 1. 1. 2009 stanovena dle nařízení vlády č.449/2008 Sb. Částku je stanovena na 3804Kč, což odpovídá nájemnímu bytu pro jednu osobu v obci od 50000 do 99999 obyvatel. Tato částka je stanovena bez ohledu na to, v jaké obci zaměstnanec bydlí.

Nezabavitelná částka se skládá z:

a) Základní nezabavitelná částka

- Dvě třetiny součtu životního minima a normativních nákladů na bydlení:
$$\frac{(3126 + 3804) \cdot 2}{3} = 4620Kč$$

[54] CIM – čistá mzda,

- Na každou další osobu, které je povinen poskytovat výživné 25%:
  $4620 \cdot 025 = 1155Kč$
  - Na manželku 1155Kč i pokud má samostatní příjem
  - Na dítě 1155Kč (může se počítat obou manželů zvlášť)

b) 1/3 zbytku čisté mzdy, maximálně však 2310Kč

Při výpočtu srážek se musí od čisté mzdy odečíst základní nezabavitelná částka. Výsledná částka se zaokrouhli směrem dolů tak, aby tato částka byla dělitelná třemi. Částka se nezaokrouhluje, pokud zbytek čisté mzdy po odečtení nezabavitelné částky je větší než součet částek životního minima a normativních nákladů na bydlení, tedy momentálně 6930Kč.

Částka po odečtení nezabavitelné částky se dělí třemi. Pokud částka přesahuje zmíněnou hranici životního minima a nákladů na bydlení, dělí se na třetinu jen tato maximální částka (momentálně 6930Kč, tedy třetina maximálně 2310Kč).

S třetinami a případně zbytkem čisté mzdy se pro odečet srážek ze mzdy pracuje následovně:

- První třetina na pohledávky oprávněných osob
- Druhá třetina pro přednostní pohledávky, pokud nejsou, dostane zaměstnanec
- Třetí třetinu dostane vždy zaměstnanec

Zbytek čisté mzdy nad stanovenou hranici 6930Kč (minimální hranice životního minima a částka nákladu na bydlení) je možné srážet bez omezení. Touto částkou se přednostně uhrazují přednostní pohledávky. Pokud zbudou finanční prostředky, uhradí se pohledávky oprávněných osob.

Přednostní pohledávky:

- Výživné
- Náhrada škody – poškození na zdraví
- Náhrada škody vzniklé trestným činem
- Poplatky, daně
- Náhrada přeplatků na dávkách (nemocenské, atd.)
- Sociální a zdravotní pojištění
- Potřeby dítěte v pěstounské péči

Příklad:

Ženatý zaměstnanec má mzdu 17500Kč a vyživuje dvě děti. Na další dvě dětí platí výživné dle soudní exekuce ve výši 2100Kč. V hlavním poměru dostává měsíční mzdu 15000Kč. Má sepsanou dohodu o srážkách na splácení dluhu u banky v hodnotě 200tisíc. Jaká mzda bude zaměstnanci vyplacena?

Základní nezabavitelná částka (Kč):

$$CZNC = ZNC + DZNC + (2 \cdot DZNC) = 4620 - 1155 + (2 \cdot 1155) = 8085$$ [55]

Zbývající čistá mzda činí (Kč): $ZCIM = CIM - CZNC = 17500 - 8085 = 9415$ [56]

Třetina zbývající čisté mzdy (Kč): $TZCIM = \frac{ZCIM}{3} = 3138{,}33$ [57]

Zaokrouhlení na stovky dolu (Kč): $TZCIM = 3138{,}33 = 3100$

Částka překračuje maximální hodnotu 1/3 2310Kč. Bude tedy stanovená maximální hodnota2310Kč a zbytek čisté mzdy (odečtení 3x 2310 = 6930Kč).

Zbytek čisté mzdy (Kč): $ZBCM = ZCIM - MH = 9415 - 6930 = 2485$ [58]

Vyřízení před. pohledávky – výživné (Kč): $VPP = TH - PP = 2310 - 2100 = 200$ [59]
(další přednostní pohledávka není, takže zbytek ke mzdě zaměstnance)

Pro vyřízení půjčky lze použít celou třetinu stanovenou pro vyřízení pohledávky oprávněné osobě. Dále lze k tomuto účelu využít zbytek čisté mzdy.

Vyřízení pohledávky - půjčka:

$$VPOO = TH + ZBCM = 2310 + 2485 = 4795$$ [60]

Zaměstnanci bude vyplaceno:

$$KV = CIM - PP - VPOO = 17500 - 2100 - 4795 = 10605$$ [61]

2.14 Postup pro výpočet mzdy

První částí pro výpočet mezd je stanovení nárokových složek mzdy – stanovení hrubé mzdy. Hrubá mzda zaměstnance je součet všech složek, které přísluší zaměstnanci za odvedenou práci. Do této práce se započítává vždy práce za odpracovaný kalendářní měsíc. Taky je potřeba brát ohledy na podmínky, které jsou uvedené v pracovní smlouvě. Do hrubé mzdy spadá:

- Základní hodinová nebo měsíční mzda

[55] CZNC – celková nezabavitelná částka, ZNC – základní nezabavitelná částka, DZNC – nezabavitelná částka pro další osoby, které je povinen poskytnout výživné
[56] ZCIM – zbývající čistá mzda
[57] TZCIM – třetina zbývající čisté mzdy
[58] ZBCM – zbytek čisté mzdy, MH – maximální hodnota stanovení zabavitelné částky
[59] VPP – vyřízení přednostní pohledávky, TH – třetina hodnoty pro sřážky, PP – přednostní pohledávka
[60] VPOO – vyřízení pohledávky oprávněné osobě
[61] KV – k výplatě

- Příplatky za práci přesčas, pohotovost, stižené pracovní prostředí, atd.
- Náhrada mzdy za svátky, dovolenou, přesčas, atd.
- Odměny, osobní ohodnocení, prémie
- Dávky nemocenského pojištění

Pokud máme stanovenou hrubou mzdu, můžeme přejít do druhé části výpočtu mezd a to je odpočtení srážkových položek. Pokud zaměstnanec pobírá naturální mzdu, musíme ještě před odpočítáváním srážkových položek připočíst tuto naturální mzdu k hrubé mzdě a vzniká zdanitelný příjem.

Veškeré dílčí výpočty byly uvedeny v předcházejících kapitolách. V předcházejících kapitolách je uveden výpočet příplatků a náhrady mezd. Pro odpočet srážkových položek je uvedeno sociální a zdravotní pojištění pro zaměstnance i zaměstnavatele, daně a ostatní srážky ze mzdy. Proto následně uvedu pouze komplexní příklad.

Příklad:

Zaměstnanec má 40hodinový pracovní týden a pravidelnou pracovní dobu. Zaměstnanec je ženatý a má dvě děti. Pobírá měsíční mzdu 15000Kč.Na jedno dítě platí výživné dle soudní exekuce ve výši 500Kč. Od zaměstnavatele má služební auto a tudíž pobírá naturální mzdu 5490Kč za auto. Fond pracovní doby je 168hodin včetně dvou svátků, které připadají na pracovní den. Zaměstnanec jeden svátek nepracoval a druhy svátek odpracoval 8hodin. Také odpracoval 10hodin přesčas v pracovní dny. Zaměstnanec měl jeden den dovolené a pět dní byl nemocný v pracovní dny. Za měsíc dostal prémii 1000Kč. Má podepsané prohlášení k dani a využívá slevu na poplatníka. Dále využívá daňové zvýhodnění na dvě děti. Průměrný hodinový výdělek pro náhradu činí 85,669Kč. Jaká mzda bude zaměstnanci vyplacena?

Zaměstnanec odpracoval (fond – dovolena – nemoc + přesčas) v hodinách:

$$OC = FPD - (DD \cdot PD) - (ND \cdot PD) + OPP = 168 - (5 \cdot 8) - (1 \cdot 8) + 10 = 130$$ [62]

Mzda za odpracovanou dobu (Kč): $OM = \frac{ZM}{FPD} \cdot OC = \frac{1500}{168} \cdot 130 = 11608$ [63]

Dovolená (Kč): $NMD = (ND \cdot PD) \cdot PHV = (1 \cdot 8) \cdot 85{,}669 = 686$

Druhý svátek pracoval – příplatek (Kč): $PPS = OS \cdot PHV \cdot PPPS = 8 \cdot 85{,}669 \cdot 1 = 686$

10 hodin přesčas – příplatek (Kč): $PPP = OPP \cdot PHV \cdot PPPP = 10 \cdot 85{,}669 \cdot 0{,}25 = 215$

Prémie (Kč): $P = 1000$

[62] FPD – fond pracovní doby

[63] OM – mzda za odpracovanou dobu

Hrubá mzda (Kč):
$$HM = OM + NMD + PPS + PPP + P = \\ = 11608 + 686 + 686 + 215 + 1000 = 14195$$

Zdanitelný příjem (Kč):
$$ZP = HM + NM = 14195 + 5490 = 19685$$

Zdravotní pojištění zaměstnanec (Kč):
$$ZPZ = ZP \cdot 4{,}5\% = 19685 \cdot 0{,}045 = 886$$

Pojištění sociální – zaměstnanec (Kč):
$$CPZ = ZP \cdot 6{,}5\% = 19685 \cdot 0{,}065 = 1280$$

Pojištění zdravotní – zaměstnavatel (Kč):
$$ZPF = ZP \cdot 9\% = 19685 \cdot 0{,}09 = 1772$$

Pojištění sociální – zaměstnavatel (Kč):
$$CPF = ZP \cdot 25\% = 19685 \cdot 0{,}25 = 4922$$

Základ daně (Kč):
$$ZD = ZP + CPF + ZPF = \\ = 19685 + 4922 + 1772 = 26400$$

Daň před zvýhodněním (Kč):
$$DPZ = ZD \cdot 15\% = 26400 \cdot 0{,}15 = 3960$$

Záloha na daň z příjmu (nemůže být záporná v Kč), DZ – 2x dítě, SD - poplatník:
$$ZDZP = DPZ - SD - DZ = 3960 - 2070 - (2x890) = 110$$

Daňový bonus (pokud po odečtení daňového zvýhodnění je ZDZP záporná v Kč):
$$DB = DPZ - SD - DZ = 4020 - 3960 - (2x890) = 110, tedy\ bonus\ \ 0$$

Náhrada mzdy na nemoc (PHV spadá pouze do první redukované hranice)

I hranice 90% (Kč):
$$I.HRPV = PHV \cdot 90\% = 85{,}669 \cdot 0{,}9 = 77{,}102$$

Redukovaný průměrný výdělek činí (Kč):

$$RPHV = I.HRH + II.HRH + III.HRH = 77{,}102 + 0 + 0 = 77{,}102$$

Náhrada za první tři dny jen v případě karantény. V tomto příkladu karanténa není, tedy náhrada mzdy za první tři nenáleží.

Denní hodinová náhrada mzdy při pracovní neschopnosti nad tři dny (Kč):

$$HNMN = RPHV \cdot 60\% = 77{,}102 \cdot 0{,}6 = 46{,}261$$

Náhrada mzdy za další dny (Kč):

$$NMN = ND \cdot PD \cdot HNMN = (5 - 3) \cdot 8 \cdot 46{,}261 = 740{,}176 \cong 741$$

Čistá mzda (Kč):

$$CIM = HM - ZPZ - CPZ - ZDZP + NMN = 14195 - 886 - 1280 - 110 + 741 = 12660$$

Základní nezabavitelná částka (poplatník + manželka + 2 děti) v Kč:
$$CZNC = ZNC + DZNC + (2 \cdot DZNC) = 4620 - 1155 + (2 \cdot 1155) = 8085$$

Zbývající čistá mzda činí (Kč):

$$ZCIM = CIM - CZNC = 12660 - 8085 = 4575$$

Třetina zbývající čisté mzdy (Kč): $TZCIM = \frac{ZCIM}{3} = \frac{4575}{3} = 1525$

Zaokrouhlení na stovky dolu (Kč): $TZCIM = 1525 = 1500$

Vyřízení před. pohledávky – výživné (Kč): $VPP = TH - PP = 1500 - 500 = 1000$ (další přednostní pohledávka není, takže zbytek ke mzdě zaměstnance)

Zaměstnanci bude vyplaceno (Kč): $KV = CIM - PP - VPOO = 12660 - 500 = 12160$

2.15 Programy pro zpracování personální a mzdové agendy

Zpracování personální a mzdové agendy můžeme rozdělit do dvou skupin. První skupinu tvoří programy, které nám slouží pro tuto evidenci. Do druhé skupiny můžeme zařadit outsourcingové mzdové účetnictví. Outsourcingové účetnictví nám může snížit mzdové náklady režijních pracovníků (mzdová účetní). Tímto můžeme taky odlehčit účetním, které se mohou specializovat na svoji práci. Dále snižujeme náklady na hardwarové a softwarové vybavení, prostory, vzdělávání pro mzdovou a personální agendu. Pro některé firmy může být vhodné poradenství, přenesení odpovědnosti za případné chyby a zastupování při jednání s potřebnými úřady.

Přehled programů pro mzdovou a personální agendu

Pro přehled programů jsem vybral programy: Duna/mzdy[64], Mzdy 2008[65], OK mzdy[66], Ekonomický software varia[67], PC mzdy[68], Pamica 2008 - pohoda[69], Money S3[70], Ježek software - účto[71] a outsourcingové mzdové účetnictví. Srovnání těchto programů je umístěno v příloze. Dále v příloze jsou tabulky podpory (školení, technická podpora), systémových požadavku a licenčních podmínek.

[64] http://www.tco.cz/
[65] http://www.ainex.cz/
[66] http://www.oksystem.cz/
[67] http://variasoft.cz/
[68] http://pcmmzdy.cz/
[69] http://www.stormware.cz/
[70] http://www.money.cz/
[71] http://www.ucto2000.cz/

3 Bezpečnost informačních systému

3.1 Bezpečná komunikace

Na bezpečnostní politiku informačního systému jsou kladeny stále větší požadavky. V počátku internetu informační systémy vznikaly převážně na akademické půdě, kde si uživatelé navzájem důvěřovali. V dnešní době velkého rozvoje internetu pro velkou škálu uživatelů se stala výměna informací v elektronické podobě trendem dnešní doby. Novým problémem se tedy stává zabezpečení výměny informací v prostředí internetu. Ne všechny informace jsou určeny pro všechny. Například informace ve státní sféře, obchodu, bankovnictví, zdravotnictví a podobně je nutné zabezpečit, aby byly důvěryhodné stejně jako při návštěvě daného institutu (osobní kontakt) a to včetně ověření totožnosti, podpisů a podobně.

Aby se IS[72] stál důvěryhodný, musí splnit řadu podmínek. Pro zajištění důvěryhodného systému existuji mezinárodní normy (ITSEC[73] a ITSEM[74]) kde jsou definovány základní bezpečnostní cíle, které systém musí splňovat. Hlavní cíle těchto norem jsou:

- **Důvěrnost informací** – zabezpečení systému proti přístupu k důvěrným informacím prostřednictvím neautorizovaného subjektu.
- **Integrita** – zabezpečení informací systému proti neautorizované modifikaci.
- **Neodmítnutelnost odpovědnosti** – informační systém musí přesvědčit třetí nezávislou stranu o přímé odpovědnosti za odeslání nebo přijetí zprávy.

Dále bývalé ministerstvo informatiky ČR v červenci roku 2000 vydalo metodickou příručku pro zabezpečování produktů a systémů budovaných na bázi informačních technologií. Tato metodická příručka se zabývá taky normou ITSEC. Tuto příručku jsem zařadil do příloh pod názvem bezpecnost.pdf [75].

3.2 Autentizace[76]

Autentizaci můžeme definovat jako proces, který nám slouží ke kontrole totožnosti uživatele. Z historie se postupně vyvinuly tři způsoby autentizace počítačového systému:

- Znalost – můžeme se autorizovat něčím, co víme (například heslo, PIN[77], …)´

[72] IS – informační systém (Information System)
[73] ITSEC – Information Technology Security Evaluation Criteria
[74] ITSEM – Information Technology Security Evaluation Manual
[75] Příručku lze stáhnout na http://www.mvcr.cz/
[76] Autentizace – ověření identity

- Vlastnictví – můžeme se autorizovat něčím, co vlastníme (například mobil, čipová karta, …)
- Biometrika – můžeme se autorizovat něčím, co je součásti naší osoby (například prst, oko, DNA[78]…)

Dnes nejpoužívanější autentizace pomocí uživatelského jména a hesla je dosti náchylné k odposlechům, znovupoužití uživatelského jména a hesla v jiných systémech a podobně. Proto jsou vhodné kombinace těchto zabezpečení. Dnes se začíná v širší míře používat zabezpečení tím, co vlastníme a autentizace něčím, co je součástí naší osoby, je spíše ještě otázkou budoucnosti. Obecně platí, že čím větší míra zabezpečení, tím je potřeba pro její prolomení být agresivnější (např. uříznout prst).

3.3 Autentizační metody

Uživatelská jména a hesla

Tento v dnešní době základní systém je založen na uživatelských účtech. Každý uživatel, který má uživatelský účet je identifikován uživatelským jménem (login) a heslem (password) chránící před neoprávněným přístupem. Pro přístup k IS tedy musíme znát uživatelské jméno a heslo. Při vstupu do IS zadáváme heslo, podle kterého počítač ověří naši totožnost a pokud se shoduje, tak nám následně poskytne přístup do systému. Jediná ochrana při zadávání hesla je, že je psané heslo překrývané hvězdičkami. To nám zabezpečuje heslo před zraky dalších lidí. U těchto systémů je třeba klást důraz na správně zvolené heslo. Taky je nutné správně hesla v systému chránit.

Volba hesla

I když heslo je základní prvek autentizačných metod, řada uživatelů nevolí dostatečně silné heslo. Následně dochází k snadnému prolomení hesla. Proto je důležité se řídit určitými pravidly. Pro dosažení nejlepšího heslo jsou:

- Používat malá a velká písmena
- Používat kromě písmen i čísla
- Používat interpunkční[79] znaky
- Dále to mohou být mezery nebo řídicí znaky

[77] PIN – osobní identifikační číslo (Personal Identification Number)
[78] DNA – genetický zápis buňky (Deoxyribonucleonicacid)
[79] interpunkční znaky – též členicí znaky

- Delší než 6znaků
- Snadno k zapamatování – aby nebylo nutno zapisovat
- Rychle a snadno k zapsání (do kolonky pro heslo)

Většina uživatelů v dnešní době je registrována u více IS. Většina těchto uživatelů volí stejné heslo pro tyto systémy nebo alespoň pro nějakou skupinu systému. Toto je zásadní problém bezpečnosti. Pokud dojde k zcizení hesla nebo k prolomení ochrany jednoho ze serveru, může se útočník pokusit pomocí zcizených hesel dostat do jiných IS. Proto se nedoporučuje používat stejné hesla. Problém nastává v tom, že většina uživatelů si nechce pamatovat řadu hesel. Pro tyto uživatele je následující doporučení. Je třeba vytvořit řadu hesel, které se dobře pamatují. Pro tyto účely se hodí vhodně modifikovat heslo. Za vhodnou modifikaci lze zvolit například počáteční (koncové) písmeno daného IS a přidat ho k heslu jako prefix[80] (sufix[81]). Např. máme heslo *poloautomat* a přihlašujeme k serveru *idnes*. Tak zvolíme heslo *poloautomati*. Pro server *krbykamna* zvolíme heslo *poloautomatk*. Těchto modifikačních pravidel je možno zvolit velké množství a je vhodné si nějaká zvolit.

Dále uživatel může být registrován v důležitých IS. Do této skupiny můžeme zařadit třeba internetové bankovnictví nebo systém našeho zaměstnavatele a podobně. Pro tyto systémy, je doporučeno z hlediska bezpečnosti nedělat modifikace hesla (a v žádném případě používat stejné heslo jako někde v jiném IS) ale zvolit jedinečné heslo pro daný systém.

Jednorázové hesla

Jedná z metod jak minimalizovat zneužití hesla, zvolení špatného hesla a pamatování si hesla, je takzvané jednorázové heslo. Tato hesla nelze použít vícekrát pro opakovatelnou autentizaci. Pokud by došlo během přenosu k odposlechu cizí osobou, bylo by mu k ničemu neboť toto heslo nelze dále než jednou použít. Vícenásobné použití může být také kontrolou, že není v přenosu něco v pořádku. Pro tento princip se využívá externí software nebo hardware, který dynamicky generuje jednorázové heslo. Při přístupu k IS je nám k dispozici zobrazené číslo, které opíšeme do programu k tomu určenému a ten nám vygeneruje jednorázové heslo. Nebo je možné k tomuto účelu použít jiné přenosné zařízení nebo kartu, na které se generují každou chvilku nová jednorázová hesla. Jednorázová hesla se taky vystavují (nebo jsou doručená poštou) jako seznam jednorázových hesel. Tento seznam se jmenuje TAN[82]. U seznamu je možnost velkého zcizení, proto se tato metoda už moc nepoužívá. Dále je v dnešní době rozšířená jednorázová autorizace pomocí mobilního telefonu.

[80] Prefix - předpona

[81] Sufix – přípona

[82] TAN – TransAction Number

Autentizace pomocí mobilního telefonu – SMS gateway[83]

Tato forma autorizace se stává čím dál víc oblíbenou. V dnešní době informačních technologií má už snad každý člověk zajímající se o internetové bankovnictví a veškeré služby spojené s internetem mobilní telefon. Proto se čím dál více lidí snaží toto využít (ať už pro SMS ankety, placené služby, jednorázově hesla, …). Výhoda této technologie je, že posíláme SMS vlastníkovi mobilní telefonní SIM[84] karty a předpokládáme, že daná osoba má telefon u sebe. Další výhoda je, že posíláme pouze jednorázové heslo s omezenou platností. Tedy nemůže za běžných okolností dojít k zcizení hesla a při každém přístupu testujeme identitu osoby.

Systém pro podporu SMS autorizace se skládá většinou ze dvou částí:

- SMS Agent
- SMS Server

SMS Agent je program, skrze kterého máme přístup pomocí SMS k datům našeho informačního systému. Nebo taky můžeme skrze něho data odesílat nebo přijímat z IS. Z hlediska autorizace je pro nás důležité automatické odesílání dat z informačního systému. SMS Agent komunikuje následně s SMS Serverem, který zajišťuje komunikaci s GSM[85] síti.

Aplikace SMS server zajišťuje komunikaci mezi SMS Agentem a GSM síti pomocí GSM terminálů. GSM server většinou vytváří už vlastní komunikaci. Tomuto programu (serveru) jsou předávané SMS zprávy. Jedná se většinou o program v GSM terminálu.

GSM terminál je hardwarové zařízení, které nám slouží k technickému odeslání nebo přijetí SMS zprávy. Jedná se zpravidla o podobné zařízení (z technického hlediska) k mobilnímu telefonu. Místo GSM terminálu je možnost použít připojení na SMS bránu našeho poskytovatele, kterému platíme za odeslané SMS. Potom je potřeba internetové připojení k poskytovateli. U nás se může jednat například o službu directsms.sluzba.cz poskytovanou společností Axima spol.s r.o[86].

SMS autorizaci bych mohl popsat následovně: v IS na serveru máme databázi uživatelů. Uživatel se přihlásí do systému pomocí uživatelského jména a hesla. Po této autorizaci a zjištění identity uživatele je mu odeslána SMS s kódem. Následně uživatel musí zadat SMS kód do systému pro potvrzení autentizace. Nebo může být požadován kód až při transakci a podobně. Pokud se jedná pro vstup do placené sekce nebo chráněné sekce, tak program může být navržen tak, že uživatel při vstupu zadá svoje SMS číslo, které následně bude ověřeno a na základě

[83] SMS gateway – SMS brána, SMS – systém krátkých GSM zpráv (Short Message Systems)
[84] SIM – účastnická identifikační karta, která slouží pro identifikaci účastníka v mobilní síti (Subscriber Information Module)
[85] GSM – globální systém pro mobilní komunikace (Global Systém for Mobile communications)
[86] http://www.axima-brno.cz/index.html

ověření odeslán SMS kód. Možností využití SMS autorizace je mnoho a záleží jen na návrhu IS a využití této technologie [22] [23] [24].

PIN

Pro autorizaci do některých systémů se také využívá zabezpečení pomocí PINů. PIN je převážně 4 až 8 místné číslo. Tuto kombinaci čísel je možno rychle odhalit, a proto se používá převážně pro zabezpečení hesel, certifikátu, platebních karet a podobně proti jejímu neoprávněnému použití. Pokud je metoda PINu použitá pro přístup do IS systému, tak se používá kombinace více bezpečnostních prvků. Např. společnost ING Group pro svůj produkt ING Konto[87] používá pro zabezpečení kromě PINu také klientské číslo a heslo [25].

Certifikáty

Zabezpečení pomocí certifikátu se dnes hojně využívá. Co to je vůbec certifikát? Certifikát by se dal přirovnat průkazu totožnosti. Tímto průkazem se subjekt prokazuje při elektronické komunikaci. Certifikát má za úkol svázat totožnost fyzickou s totožností elektronickou daného subjektu. Tato totožnost je zaručena podpisem certifikační autority. Žádající subjekt musí splňovat řadu kritérií a dodat potřebné dokumenty ověřující jeho totožnost na některou z certifikačních autorit, kde si chce nechat certifikát podepsat. Certifikát si může subjekt vystavit sám na základě dostupných programů a následně si subjekt může certifikát taky sám podepsat. Při vlastním podpisu se stává méně důvěryhodný, než kdyby ho podepsala některá ze známých certifikačních autorit. Hlavní částí certifikátu jsou údaje o subjektu, datum vypršení platnosti certifikátu, veřejný a privátní klíč.

Druhy kryptografie

Šifrovací metody můžeme rozdělit do dvou skupin:

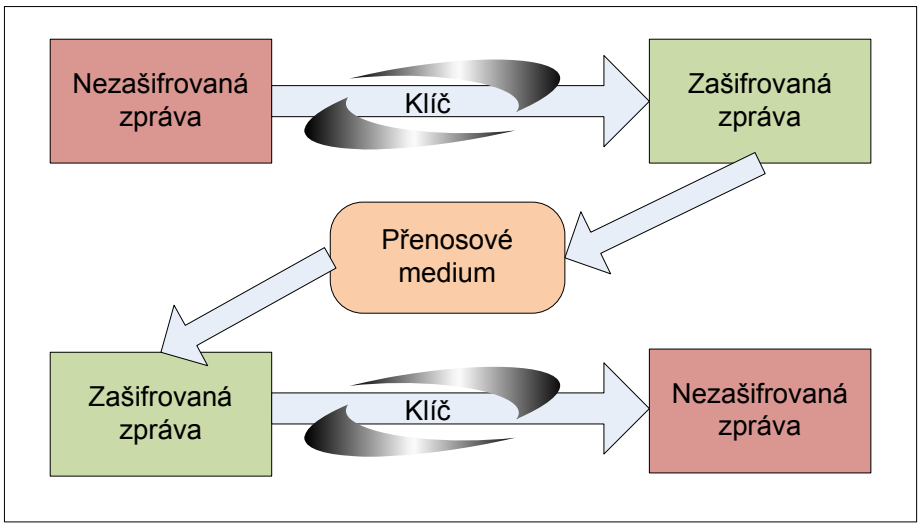
- Symetrická kryptografie
- Asymetrická kryptografie

Symetrická kryptografie

Tato metoda je postavena na principu použití stejného klíče, který byl použít pro zašifrování dat, tak i k odšifrování dat. Tedy stejný klíč je použít jak na straně odesílatele, tak i na straně příjemce. Tato metoda naráží na problém předání šifrovacího klíče druhé straně. Problém

[87] http://www.ingkonto.cz/cz/

nastává v tom, že před zahájením komunikace druhá strana nemá šifrovací klíč k odšifrování zprávy. Proto je nutno předat klíč nějakou bezpečnou metodou (osobní předání, poštou, důvěryhodný kanál, atd.).



Obrázek 2: Symetrická kryptografie

Použití symetrické kryptografie představuje způsob, jak zabezpečit důvěrnost transakcí. Tyto algoritmy neřeší požadavek neodmítnutelnosti odpovědnosti. Tedy nelze určit, která strana zprávu odeslala a která přijala.

Asymetrická kryptografie

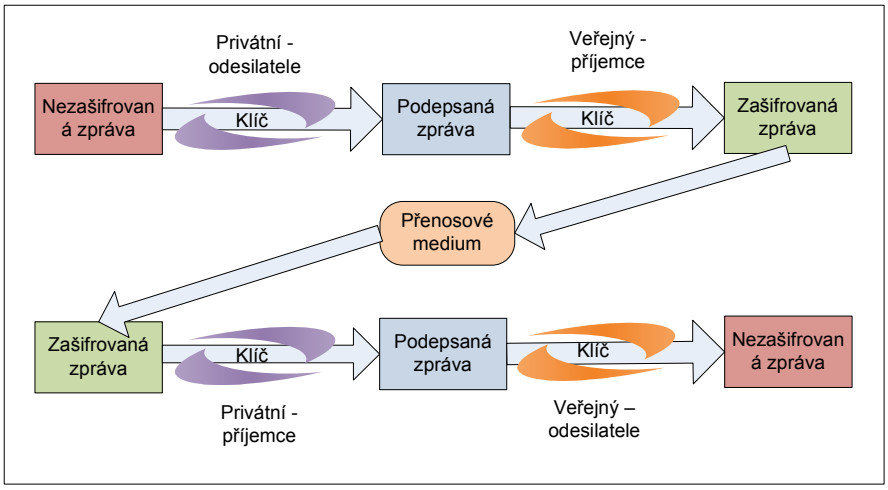
Výhoda oproti symetrické kryptografii je využívání dvojice klíčů, které jednoznačně identifikují jak odesílatele, tak příjemce. Tuto dvojici klíčů si vygeneruje uživatel pomocí nějakého dostupného programu a následně se stává jediným majitelem těchto klíčů. Tato technika je založena na principu, že data šifrována jedním z klíčů lze v rozumném čase dešifrovat jen pomocí druhého klíče a naopak.

Klíče dělíme na privátní klíč (tento klíč je bedlivě střežen majitelem) a veřejný klíč, který je zveřejněn. Pokud známe vlastníka privátního klíče, známe i odesílatele. Odesílatel privátním klíčem zprávu podepíše – zašifruje. Příjemce veřejným klíčem zprávu dešifruje. Tato zpráva není důvěrná a ani za důvěrnou ji nelze považovat z důvodu, že veřejný klíč je znám všem. Tedy tuto zprávu považujeme pouze za podepsanou.

Tímto způsobem se řeší nejčastěji integrita dat a odpovědnost ze strany odesílatele. Příjemce může následně taky poslat podepsané potvrzení o přijetí zprávy nebo odpověď. Pak je zajištěna odpovědnost i ze strany příjemce. Problém nastává při důvěryhodnosti zprávy. Každý neautorizovaný objekt si může zprávu pomocí veřejného klíče dešifrovat.

Tento problém lze vyřešit pomoci šifrování zprávy veřejným klíčem adresáta. Při zašifrování zprávy tímto klíčem máme jistotu, že zprávu přečte pouze adresát s privátním klíčem.

Celý systém šifrování zpráv v obousměrné komunikaci pracuje tedy následovně. Na straně odesílatele je čitelný text nejdříve podepsán privátním klíčem odesílatele a následně podepsaná zpráva odesílatele je šifrována veřejným klíčem adresáta. Na straně adresáta je nejprve zpráva privátním klíčem adresáta dešifrována, čímž je zajištěna adresnost zprávy a teprve potom je pomocí veřejného klíče odesílatele ověřena identita odesílatele [26] [27].



Obrázek 3: Asymetrická kryptografie

Princip a využití certifikátu – digitální podpis

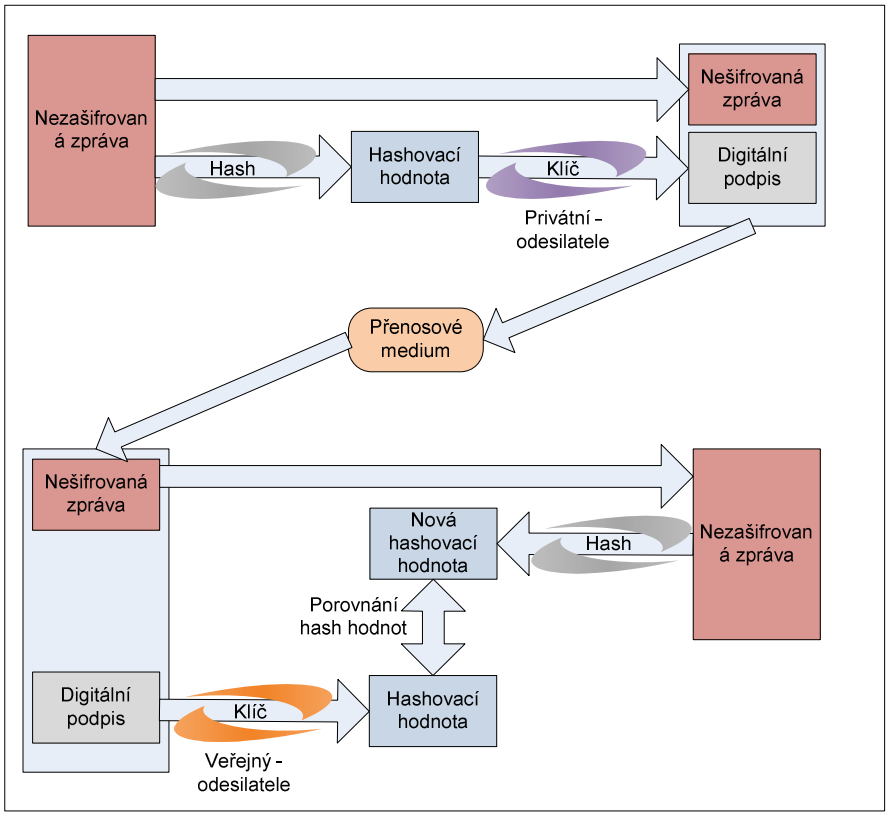
V dnešní době se většinou asymetrická kryptografie nepoužívá k šifrování celých zpráv, ale využívají se k tvorbě takzvaných digitálních podpisů dat.

Symetrická metoda kryptografie oproti asymetrické metodě má výhodu ve vyšší rychlosti algoritmu. Tato vlastnost vyplívá z podstaty matematické složitosti algoritmu asymetrické kryptografie. V reálné praxi při tvorbě podpisu se z tohoto důvodu nešifrují celá data privátním klíčem. Na celá data se nejdříve použije hashovací funkce. Hashovací funkce nám vypočte z dat hashovací hodnotu. Algoritmus pro výpočet hashovací hodnoty z dat je velmi rychlý, což je velmi výhodné oproti šifrování privátním klíčem. Někdy se této hodnotě taky říká digitální obtisk velkých dat. Důležité je, že zpětné získání dat z hashovací hodnoty je nemožné. Mezi nejznámější hashovací funkce patří například MD2[88] či MD5[89].

Při odesílání dat se tedy jako první vypočte hashovací hodnota z velkých dat. Následně se hashovací hodnota zašifruje asymetrickým algoritmem s použitím privátního klíče. Tato

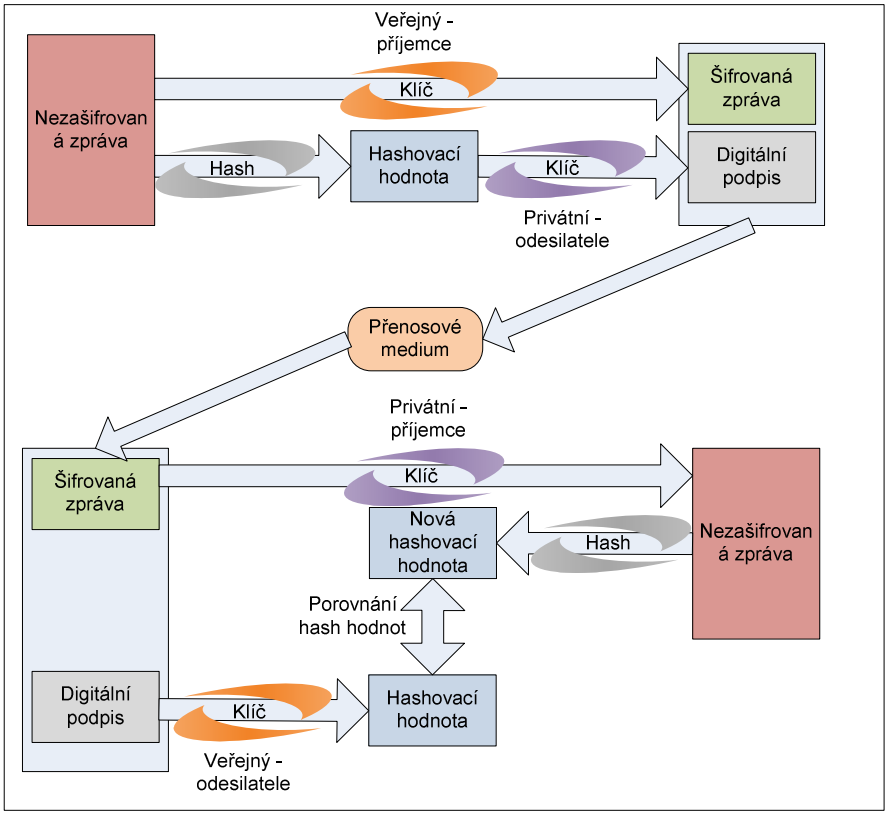
[88] MD2 – 2.protokol pro autentizací (Message Digest Algorithm 2)
[89]MD5 – 5.protokol pro autentizací (Message Digest Algorithm 5)

podepsaná hashovací hodnota se nazývá digitální podpis, která je následně odeslána jako příloha dat. Příjemce dat provede dešifrování digitálního podpisu pomocí veřejného klíče předpokládaného odesílatele. Tímto příjemce získá hashovací hodnotu. Následně musí příjemce provést vypočet hashovací hodnoty, stejnou hashovací funkci, jako použil odesílatel. Pro správnost dat se obě tyto hashovaci hodnoty musí rovnat.



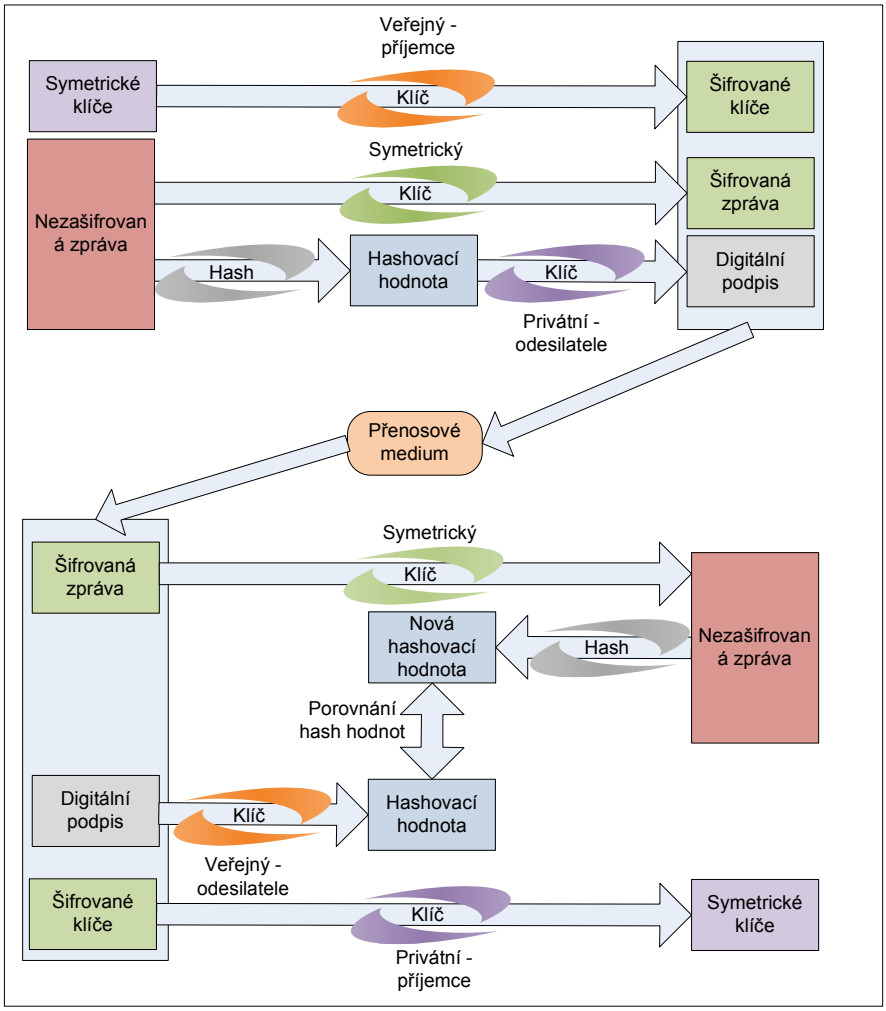
Obrázek 4: Digitální podpis

Tato metoda nám zaručuje jednoznačnou identitu a správnost posílaných dat. Problém u této metody je čitelnost dat během přenosu. Proto se používá upravena metoda, kde šifrujeme celá data. Dalo by se využít šifrování dat pomocí veřejného klíče příjemce a následně po přijetí zprávy by si příjemce pomocí svého privátního klíče data dešifroval (se stanou čitelné) a následně zkontroloval digitální podpis. Předpokládáme, že odesílatel by před zašifrování dat provedl vypočet digitálního podpisu.



Obrázek 5: Digitální podpis

Tato metoda spolehlivě chrání data během přenosu, ale naráží na problém šifrování celé zprávy pomocí asymetrických metod. Problém nastává pří šifrování velkých dat, které by na obou stranách trvalo neúměrně dlouho. Proto se začala používat modifikace této metody. Nejdříve se k datům vypočte hashovací hodnota. Z této hodnoty se pomocí asymetrických metod (privátní klíč odesílatele) vytvoří digitální podpis. Celá data se následně šifrují pomocí symetrických metod. Klíče pro symetrické šifrování dat se následně šifrují pomocí asymetrických metod (veřejný klíč příjemce), aby během přenosu nebyly čitelné. Následně se tento balík dat (klíče pro symetrické šifrování, šifrované data symetrickou šifrou a digitální podpis) odešlou příjemci dat. Ten následně postupuje v opačném pořadí. Nejprve pomocí asymetrických metod (privátní klíč příjemce) se dešifrují symetrické klíče. Pak pomocí symetrického klíče se dešifruje obsah dat. Následně se vytvoří hashovací hodnota z obsahu dat a porovná se s hashovací hodnotou v digitálním podpisu. Tato komunikace vyžaduje dohodu o formátu přenášených dat a systému jejich šifrování [26] [27] [28].



Obrázek 6: Digitální podpis

Časové razítka (Time stamp TS)

Pro řadu dokumentů nám elektronický podpis nestačí pro podepsání dokumentů. K podpisu může být potřeba připojit časové razítko pro časové určení, což je u mnoha dokumentů žádoucí. Příkladem dokumentů, pro které je časové razítko nepostradatelné, je elektronické daňové přiznání. Tento dokument musí být podaný v určitém termínu, jinak může dojít k pokutám. Proto potřebujeme jistý zdroj času, kterému můžeme důvěřovat, že je správný. Pokud bychom tento zdroj času neměli, mohl by si uživatel posunout čas zpět a podepsat dokument s nepravdivým datem. Dalším problémem, který nám řeší časová razítka je ověřování elektronických podpisů po delším časovém okamžiku od jejich vytvoření nebo archivace podepsaných dokumentů.

Časové razítko je součástí PKI[90]. U dokumentů s dlouhou dobou platnosti by šlo zpochybnit platnost podepsaného dokumentu, pokud bychom nahlásili ztrátu privátního klíče a tedy odvolali certifikát. Kdyby nebyla existence časového razítka, tak nikdo nedokáže, zda byl dokument podepsán před odvoláním certifikátu nebo až po něm. Časová razítka zaručují existenci dokumentů v daném čase. Pro poskytování elektronických notářských služeb a zajišťování archivace podepsaných dokumentů je existence autority časových razítek TSA[91] nutným základem. Časové razítko je elektronicky podepsáno (vydáváno) autoritou TSA pro vydávání časových razítek.

Časové razítko neobsahuje žádnou identifikaci žadatele. Tedy není možné určit, kdo měl dokument v držení před udělením časového razítka.

Časové razítko je strukturou podobné certifikátu. Na rozdíl od certifikátu časové razítko svazuje kontrolní součet (tedy hash z dokumentu) s časem. Elektronicky podepsaná struktura časového razítka mj. obsahuje: jméno vydavatele (jméno TSA), jedinečné sériové číslo razítka, kontrolní součet (hash) z dokumentu a čas.

Pokud potřebujeme časové razítko pro dokument, tak nejčastěji se žádá prostřednictvím klientské aplikace. Klient musí vytvořit žádost o časové razítko, což je datová struktura obsahující hash dokumentu. Tuto žádost ve standardizovaném formátu odešle do TSA. TSA v kladném případě odesílá odpověď žadateli obsahující časové razítko. Časové razítko je podepsaná standardizovaná datová struktura obsahující číslo časového razítka, hash dokumentu, čas a název vydavatele TSA [29] [30].

Certifikační autority

Certifikační autorita má za úkol vystupovat mezi komunikaci dvou subjektu v prostředí internetu jako třetí nezávislá strana pro ověření identity komunikujících objektů.

Certifikační autorita vystavuje digitální certifikáty. Vydávání certifikátu se řídí certifikační politikou. Každá certifikační autorita musí mít tento dokument, ve kterém jsou stanovené podmínky vydávání certifikátů. Pro vydání certifikátu si musí žádající objekt vygenerovat pár klíčů, a na základě informací o žadateli a klíčů je podepsán certifikát certifikační politikou, která zaručuje správnost údajů uvedených v certifikátu.

Při komunikaci pravost certifikátů ověřuje internetový prohlížeč. Prohlížeč ověřuje pravost údajů v certifikátu (jméno serveru, platnost certifikátu, a další údaje v certifikátu). Pro ověření pravosti a důvěřování datům uvedených v certifikátu slouží tzv. certifikační autorita, jíž je certifikát digitálně podepsán. Certifikační autorita ručí za správnost údajů. Pokud si může prohlížeč ověřit podpis certifikátu a dané certifikační autoritě důvěřuje (která ho podepsala),

[90] PKI – struktura veřejných klíčů – zabezpečení jedinečnosti, kryptografie (Public Key Infrastructure)
[91] TSA – autorita časové značky – vydává časové razítka (Time Stamping Authority)

může mít jistotu, že komunikuje opravdu s tím, s kým chtěl komunikovat. Pro ověření podpisu musí mít prohlížeč certifikát CA[92]. Pomocí tohoto certifikátu podpis ověří. Pokud certifikát CA, která je podepsaná v ověřovaném certifikátů, není v prohlížeči nainstalována, zahlásí prohlížeč chybu a dotáže se, zda má pokračovat v komunikaci, i když certifikátu nedůvěřuje. Pokud nechceme být otravováni hláškami od internetového prohlížeče a danému certifikátu důvěřujeme, musíme do prohlížeče doinstalovat certifikáty od CA, kterým důvěřujeme. V internetovém prohlížeči je standardně nainstalováno několik certifikátů známých CA. Většinou jsou v prohlížeči certifikáty CA té země, odkud internetový prohlížeč pochází [26] [33].

Mezi nejznámější a největší světové certifikační autority v dnešní době patří VeriSign, kterou používá většina největších světových společnosti a v oblasti financí tato certifikační autorita patří k samozřejmostem. Za další největší světovou certifikační autoritu můžeme považovat THAWTE, která je v současnosti 100% vlastníkem VeriSign. Ceny a podmínky těchto certifikátů lze zjistit například na: www.czechia.com nebo www.thawte.com. Pro názornost zde zobrazuji tabulku s cenami certifikátu VeriSign (jedná se o nové vystavené certifikáty a pouze o krátký výtažek z ceníku k 1.11.2008):

Secure Site Certifikát	
Běžný certifikát, obsahuje doménové jméno, e-mail, název organizace, organizační jednotku a umožňuje šifrování s klíčem o síle 40/56/128 bitů podle podporovaného nastavení prohlížeče.	
1 rok	450 EUR
2 roky	820 EUR
Secure Site Pro EV Certifikát	
Certifikát SSL PRO EV (EV = extended validation) je certifikát, který je v nových prohlížečích označen zelenou barvou s informací o organizaci, která vlastní tento certifikát.	
1 rok	1499 EUR
2 roky	2495 EUR

Tabulka 5: VeriSign - Secure Site Certifikát

Mezi české certifikační autority můžeme zařadit: První certifikační autorita a.s. (I.CA). Dále také například CA CZECHIA.CZ, CESNET CA, CA TrustPort a další. I.CA je jako jediná státem akreditovaná společnost u nás. Pro názornost ceny české CA I.CA k 1.11.2008:

[92] CA – certifikační autorita (Certfication autority)

Kvalifikované certifikáty		
Typ	**Popis**	**Základní cena s DPH**
Standard	Doba platnosti 12 měsíců (365 dní) Použití 1024 bitového kryptografického klíče	752 Kč
Comfort	Cena zahrnuje : certifikát - doba platnosti 12 měsíců (365 dní) - použití 1024 kryptografického klíče - čipová karta - ovládací software I.CA	1728 Kč

Tabulka 6: I.CA – kvalifikované certifikáty

Kvalifikované systémové certifikáty		
Typ	**Popis**	**Základní cena s DPH**
Standard	(žadatel má vlastní hardwarové zařízení) Doba platnosti 12 měsíců (365 dní) Použití 1024 bitového kryptografického klíče	780 Kč
Comfort	Cena zahrnuje : certifikát - doba platnosti 12 měsíců (365 dní) - použití 1024 kryptografického klíče - čipová karta - ovládací SW I.CA	1756 Kč

Tabulka 7: I.CA - kvalifikované systémové certifikáty

Komerční certifikáty		
Typ	**Popis**	**Základní cena s DPH**
Standard	Doba platnosti 6 měsíců (183 dní) Použití 512 bitového kryptografického klíče	322 Kč
Standart	Doba platnosti 12 měsíců (365 dní) Použití 1024 bitového kryptografického klíče	580 Kč
Confort	Cena zahrnuje : certifikát - doba platnosti 12 měsíců (365 dní) - použití 1024 kryptografického klíče - čipová karta - ovládací software I.CA	1556 Kč

Tabulka 8: I.CA - komerční certifikáty

Certifikát pro server		
Typ	**Popis**	**Základní cena s DPH**
	Doba platnosti 6 měsíců (183 dní) Použití 512 bitového kryptografického klíče	1073 Kč
	Doba platnosti 12 měsíců (365 dní) Použití 1024 bitového kryptografického klíče	1931 Kč

Tabulka 9: I.CA - certifikáty pro server

Pro soukromou komunikaci nebo malé projekty, které nemají zájem investovat do podpisů známých CA, mohou využít možnost vygenerovat vlastní certifikační autoritu a tou následně podepisovat certifikáty. Aby následně přijal internetový prohlížeč tyto certifikáty bez jakéhokoliv hlášení o nedůvěřování danému certifikátu, je nutné certifikát vlastní CA nainstalovat do internetového prohlížeče [31] [32].

Protokol SSL (Secure Socket Layer), TLS (Transport Layer Security)

Protokol SSL a SSL certifikáty se využívají pro bezpečnou komunikaci na internetu. Chrání komunikaci pomocí šifrování mezi klientem a serverem. Pro finanční prostředí je SLL protokol a SLL certifikáty nutností. Pro šifrovanou komunikaci v prostředí internetu se používá zmíněný protokol SSL. Pro ověření totožnosti komunikujících stran se používají certifikáty. Tyto certifikáty pro zabezpečený přenos přes SSL se taky někdy nazývají SSL certifikáty.

SSL tedy má dvě funkce. Šifrování a autentizaci pomocí certifikátu. SSL bylo vytvořeno v roce 1994 pod záštitou firmy Netscape Communication. Tento protokol je podporován většinou internetových prohlížečů a klientskými aplikacemi. Samozřejmostí je podpora serverovými aplikacemi a podpora od certifikačních autorit.

Verze SSL 2.0 umožňovala pouze autentizaci serveru. S toho plynulo, že pouze na server se instaloval certifikát. Novější a v současnosti používána verze SSL 3.0 už podporuje autentizaci klienta i serveru a vznikla v roce 1996. U této verze, pro zahájení šifrovaného přenosu, se musí prokázat certifikátem klient i server. Toto řešení vyžaduje infrastrukturu veřejných klíčů (PKI) u klientů. Verze SSL 3.0 se stála základem pro nový protokol TLS 1.0.

SSL zabezpečuje aplikační protokoly jako je TCP/IP[93], HTTP[94], TELNET[95] a podobně. SSL nám poskytuje zabezpečenou komunikaci při inicializaci TCP/IP spojení. Při této inicializaci se

[93] TCP/IP – řídicí přenosový protokol / protokol internetu (Transminnion Control Protokol / internet Protocol)

[94] HTTP – hypertextový přenosový protokol (HyperText Transfer Protocol)

[95] TELNET – Virtuální síťový terminál pro interaktivní přístup ke vzdáleným počítačům (TELecommunication NETwork)

klient a server domluví na použité bezpečnostní metodě a provedou vzájemnou autentizací pomocí certifikátu. Po této domluvě je šifrování aktivováno. SSL šifruje a dešifruje proud bitů konkrétního aplikačního protokolu. Tato bezpečnostní vrstva mezi protokoly má vliv na rychlost komunikace mezi serverem a klientem. Na druhou stránku má velký přínos v bezpečnosti. Proto se doporučuje zabezpečovat jen tu část IS, která to z hlediska bezpečnosti vyžaduje.

Vytvoření SSL spojení probíhá následovně (SSL handshake, potřásání rukou):

- Klient pošle serveru požadavek na SSL spojení.
- Server pošle odpověď na požadavek, obsahuje stejný typ informaci a certifikát serveru.
- Klient si podle certifikátu ověří autentičnost serveru. V certifikátu je také obsazen veřejný klíč.
- Následně z informací si vybere nejsilnější metody a vygeneruje klient základ šifrovacího klíče. Klient zašifruje šifrovací klíč veřejným klíčem serveru a pošle to serveru.
- Server soukromým klíčem rozšifruje šifrovací klíč. Z tohoto základního šifrovací klíče si klient i server vygenerují hlavní šifrovací klíč.
- Klient i server se následně domluví, že následná komunikace už bude šifrována hlavním šifrovacím klíčem. Potřásaní rukou končí.
- Aplikace dál už komunikují přes šifrované spojení.

Požadavek na SSL spojení obsahuje verzi SSL, nastavení šifrování atd. V první fázi si klient se serverem dohodnou kryptografické algoritmy. Dnes jsou nejpoužívanější následující volby:

- Pro výměnu klíčů: RSA[96], DSA[97], Diffie – Hellman, Fortezza
- Pro Symetrickou šifru: RC2[98], RC4[99], IDEA[100], DES[101], 3DES[102], EAS[103]
- Pro jednocestné hašovací funkce: MD5, SHA[104]

[96] RSA – autoři algoritmu (Rivest Shamir Adleman)
[97] DSA – algoritmus (Digital Signature Algorithm)
[98] RC2 – autor Ronald Rivest,blokový algoritmus
[99] RC4 – autor Ronald Rivest, proudová verze RC2
[100] IDEA – algoritmus pro šifrování (International Data Encryption Algorithm)
[101] DES - algoritmus pro šifrování (Data Encryption Standard)
[102] 3DES - algoritmus pro šifrování (Triple Data Encryption Standard)
[103] EAS – algoritmus pro šifrování (Advanced Encryption Standard)
[104] SHA – hešovací algoritmus (Secure Hashing Algorithm)

TLS (Transport Layer Security) je vytvořen v rámci IETF[105] jako internetový standart a má za úkol nahradit protokol SSL 3.0. Protokol TLS 1.0 je založen na specifikaci protokolu SSL 3.0. Rozdíly mezi TLS 1.0 a SSL 3.0 jsou malé, ale jsou natolik významné, že protokoly spolu nespolupracují.

Rozdíl TLS 1.0 a SSL 3.0 je hlavně v délce šifrovacího doplňku. Tedy jestliže před šifrováním šifrovaná data mají délku 79byte a délka šifrovacího bloku je 8, pak doplněk může být dlouhý 1, 9, 17, … , 249byte. U SSL byl doplněk nejkratší možné velikosti tedy v našem příkladě 1byte. Použití této metody proměnné délky doplňku stěžuje útok pomocí analýzy délky zpráv. Oproti SSL dále neobsahuje výstrahu *no_certifiate* a výměnu klíčů typu *Fortezza*. Rozdíl oproti SSL je taky ve výpočtu MAC[106], ale výsledná úroveň zabezpečení je shodná. Poslední větší drobný rozdíl je ve zprávách typu *certificate_verify* [27] [34] [35] [36].

Generování certifikátu

Pro generování certifikátu můžeme využít kryptografický nástroj Open SSL. Tento nástroj implementuje Secure Socket Layer (SSL v2/v3) a Transport Layer Security (TLS v1) a další přidružené kryptografické standarty. Tento nástroj pracuje v příkazové řádce a využívá funkce z knihovny krypto, která je napsaná v jazyce C.

Open SSL lze využít pro:

- Vytváření X.509 certifikátů
- Vytváření RSA, DH a DSA klíčů
- Počítání výtahů zpráv
- Šifrování a dešifrování
- SSL/TLS – testování klienta a serveru
- Podepisování, šifrování, dešifrování a verifikace e-mailů

Vytvoření certifikační autority

Zde máme možnost si buď nechat certifikát podepsat známou certifikační autoritou (důvody viz kapitola Certifikační autorita) nebo máme možnost vytvořit vlastní certifikační autoritu a následně s touto CA podepisovat certifikáty. Tato možnost se volí většinou u firemních sítí, kde následně nainstalujeme CA na jednotlivé stanice. U veřejného serveru by nebylo vhodné nutit všechny uživatele, aby si instalovali certifikát naši CA.

[105] IETF – skupina podílející se na rozvoji internetu (Internet Engineering Task Force)
[106] MAC – autentizační kód zprávy (Message Autentication Code)

Pro generování certifikátu CA musíme vytvořit adresář pro certifikační autoritu (adresář = jméno CA). V něm následně vytvoříme potřebné základní podadresáře: *certs* (adresář pro vydané certifikáty, např. *CCA_CA*), *crl* (adresář pro crl – zrušené certifikáty), *newcerts* (implicitní adresář pro nové certifikáty), *private* (uchování soukromých dat CA), *private/keys* (vygenerované privátní klíče uživatelů), *private/certsp12* (certifikáty uživatelů PKCS#12[107]) , *requests* (pro uchování požadavků o certifikáty). Dále vytvoříme prázdný soubor *index.txt* (textová databáze vydaných certifikátů) a soubor *seriál* s obsahem 01 (soubor s aktuálním sériovým číslem následného certifikátu). Před generováním je nutné upravit konfigurační soubor [27] [36] [37].

Následně potřebujeme upravit konfigurační soubor openssl.cnf:

dir = ./CCA_CA

certs = $dir/certs

crl_dir = $dir/crl

database = $dir/index.txt

new_certs_dir = $dir/newcerts

certificate = $dir/cacert.pen

serial = $dir/serial

crl = $dir/crl.pem

private_key = $dir/private/cakey.pem

RANDFILE = $dir/private/ .rnd

Do složky *private* zkopírujeme soubor *.rnd* s adresáře *open_ssl*. Dále je nutno v této složce vytvořit soubor *keypasswd.info* s implicitním heslem pro použití privátního klíče.

Následně můžeme vygenerovat privátní klíč CA:

openssl genrsa -out ./CCA_CA/private/cakey.key 1024

Následně vytvoříme certifikát pro naší CA. Zde můžeme zadat jeho časovou platnost – v příkladě 2roky(tedy 730dní):

openssl req -x509 -new -key ./CCA_CA/private/cakey.key -out

./CCA_CA/cacert.pem -config ./config/openssl.cnf –days 730

Pro instalaci certifikátu do prohlížeče je nutno převést certifikát z formátu PEM[108] do DER[109].

[107] PKCS#12 – PKCS – Public Key Cryptography Standart, PKCS#12 – Personal information Exchange Syntax Standart

[108] PEM – formát certifikátu

openssl x509 -in ./CCA_CA/cacert.pem -inform PEM -out ./CCA_CA/cacert.der –

outform DER

Je vhodné také vytvořit počáteční CRL[110]:

openssl ca -gencrl -config ./CCA_CA/openssl.cnf -out ./CCA_CA/crl/crl.pem

Vytvoření certifikátu severu

Nejprve vytvoříme privátní klíče (argument *passout* pro automatické načtení hesla ze souboru):

openssl genrsa -out ./CCA_CA/private/keys/server.key -passout

file:./CCA_CA/private/keypasswd.nfo 1024

Vytvoření požadavku na certifikát:

openssl req -new -key ./CCA_CA/private/keys/server.key -out

./CCA_CA/requests/server.req -config ./CCA_CA/openssl.cnf

Během běhu tohoto příkazů postupně vyplňujeme údaje, které ve výsledku tvoří DN (Distingish Name) serveru. Je nutná shoda DN s doménou serveru. V seznamu *index.txt* se nám vytvoří nový záznam s údaji o vytvořeném certifikátu.

Jako poslední příkaz je nutné podepsat certifikát CA:

openssl ca -in ./CCA_CA/requests/server.req -out

./CCA_CA/certs/servercert.pem -config ./CCA_CA/openssl.cnf

Vytvoření certifikátu uživatele

Nejprve vytvoříme privátní klíč (jako u certifikátu serveru):

openssl genrsa -out ./CCA_CA/private/keys/user01.key -passout

file:./CCA_CA/private/keypasswd.nfo 1024

Následně vytvoříme požadavek na certifikát:

openssl req -new -key ./CCA_CA/private/keys/user01.key -out

./CCA_CA/requests/user01.req -config ./CCA_CA/openssl.cnf -subj

"/C=CZ/ST=Czech Republic/O=Mirek a syn s.r.o/CN=Mirek Hlosta" –batch

Následně musíme zase podepsat certifikát CA:

---

[109] DER – formát certifikátu

[110] CRL – seznam zneplatněných certifikátů (Certificate revocation list)

openssl ca -in ./CCA_CA/requests/user01.req -out ./CCA_CA/certs/user01.pem

-config ./CCA_CA/openssl.cnf –batch

Pro import do prohlížeče budeme muset certifikát převést do formátu PKCS#12:

openssl pkcs12 -export -in ./CCA_CA/certs/user01.pem -inkey

./CCA_CA/private/keys/user01.key -out ./CCA_CA/private/certsp12/user01.p12

Čipové karty

Čipové karty pro autentizaci se většinou používají jako prostředí pro uložení kryptografického klíče. Čipové karty lze rozdělit na dvě skupiny:

- Pasivní čipové karty

Čipová karta slouží pouze pro uchování informace, tudíž data jsou zpracována vnější aplikací. Tyto karty tedy nesplňují bezpečnost, kterou nám nabízí aktivní čipové karty a kterou od těchto karet očekáváme.

- Aktivní karty

Tyto karty obsahují kromě dat (např. kryptografického klíče) taky aplikaci, která data využívá. Vnější aplikace používají tyto informace pouze zprostředkovaně. Tajná data čipovou kartu neopouštějí a tedy nemůže být zneužita se zařízením, s nímž karta komunikuje.

U aktivní čipové karty jsou veškeré podstatné kryptografické operace prováděny přímo v čipové kartě. Tato karta vytváří autonomní jednotku nebo veškeré algoritmy pro ověření či vytvoření digitálního podpisu jsou uloženy na ní.

Z technického hlediska čipové karty obsahují mikroprocesor a paměť uchovávající kryptografický klíč. Tyto osobní klíče jsou uloženy přímo na kartě a jsou chráněny mikroprocesorem. Mikroprocesor obsahuje algoritmus (např. RSA, DSA, …) pro podepisování operací a kódování. K těmto účelům (kódování, podepisování) nám slouží klíč uložený v paměti na kartě. Algoritmus provádí kryptografické operace s daty, která mu byla zaslána. V dnešní době minimální délka klíčů na kartě je okolo 1024bitů, ale tento parametr stále roste stejně jako velikost paměti na kartě.

U nás čipové karty a čtečky karet nabízí řada společností například společnost COMPELSON Trade s.r.o. Tato společnost nabízí několik druhů profesionálních mikroprocesorových asymetrických a kryptografických PKI čipových karet.

Karty jsou chráněny proti zcizení nebo ztrátě pomocí PINu nebo majitel musí jinak prokázat svojí identitu k kartě (například obtisk prstu) [21] [38] [39].

USB[111] token

Někdy taky čipové tokeny. Tyto tokeny jsou standardně připojitelné do USB portu počítače a tudíž kombinují čipovou kartu a čtečku čipové karty v jednom objektu hardware. Většina USB tokenu se podobá USB flash diskům, ale nelze je zaměňovat. Oproti flash diskům pracují na principu čipové karty. Tedy obsahují mikroprocesor a paměť. Z této technologie plyne, že nelze přistupovat přímo k citlivým datům na tokenu. Vlastnosti tokenu jsou srovnatelné s čipovou kartou, ale výhoda oproti kartám je v jejich velikosti (je možné připojit na důležitou věc, aby nedošlo k jeho zapomenutí v počítači) a mobilitě (není nutné přenášet čtečku karet, jak je zapotřebí u čipové karty).

S použitím čipových karet a tokenů se někdy zavadí pojem dvoufaktorová autentizace (two-factor authentication) . Tato autentizace si klade za cíl nějakou znalost (např. PINu) nebo vlastnost biometriky(např. obtisk prstu) a také držení čipové karty nebo tokenu [21] [38].

Biometrika

Autorizace pomocí biometriky nám řeší problém s pamatováním hesel, ukládání a přenos certifikátu, atd. Tato metoda se převážně používá pro přístup do střeženého prostoru a podobně. Při neustálém zlevňování čteček na obtisku prstu se tato metoda začíná čím dál více používat pro zabezpečení všedných věcí. Tato metoda je na úrovni zabezpečení pomocí hesel a PINu. Dnešní nejpoužívanější metody jsou asi kombinace čipové karty (zde uložen například certifikát) s některým z biometrických údajů o oprávněném uživateli. Za biometrické prvky můžeme považovat charakteristické prvky lidských jedinců pro jejich rozpoznání, jako je obtisk prstů, geometrie ruky, zabarvení lidského hlasu, tvar obličeje, oční sítnice, analýza DNA, apod. Některé tyto znaky jedince jsou rozpoznatelné tak přesně, že mohou sloužit k jeho identifikaci s ověřením identity (autentizace). Nejčastěji se používá obtisk prstů, ruky či struktura oka.

Největší výhoda těchto biologických znaků je, že je nosíme stále s sebou, nemůžeme je nikde zapomenout či ztratit a jsou těžko rozkódovatelné či padělatelné. Problém by nastal v situaci, pokud by se někomu podařilo například obtisk prstu sejmout a replikovat. Zde by nastal s obtiskem problém s prohlášením za neplatný. Nelze vytvořit jako u certifikátu seznamu zneplatněných certifikátů (CRL). Tzv. nelze revokovat biometrický prvek.

V dnešní době největšího využití biometriky, s možným využitím v internetovém prostředí, je ochrana údajů na čipových kartách. Pokud chceme získat údaje z čipové karty (např. privátní klíč) v čtečce čipových karet vybavené snímačem obtisků, musíme přiložit prst k čtečce karet a ta nám následně ověří naši identitu a na základě rozhodnutí povolí, či zamítne přístup na čipovou kartu. Většinou se veškeré šifrování provádí už jen na čipové kartě z důvodu, aby data (např. privátní klíč) neopustila čipovou kartu a nedošlo k jejím zkopírování uvnitř počítače.

[111] USB – univerzální sériová sběrnice (Universal Seriál Bus)

Z hlediska bezpečnosti je vhodné používat zařízení, která kombinují biometrickou vlastnost se čtečkou čipových karet. Při oddělení těchto dvou zařízení může dojít k zaútočení na váš počítač a získání vzorku. Není vhodné ukládat vzorky datových obtisků na serveru [40].

3.4 Bezpečnostní politika firem

V dnešní době velkého rozmachu informačních technologií, stoupá taky nebezpečí ztráty dat z podnikových sítí a systémů. Na toto nebezpečí reaguje řada firem, která se snaží zabezpečit tyto firmy proti zcizení firemních dat. I když existuje celá řada softwarových i drahých a kvalitních hardwarových firewallu[112], největší nebezpečí hrozí z vnitřku firmy. Tedy největší zranitelnost bezpečnosti IT je v lidském faktoru. Tato nebezpečí nemusí přímo způsobovat zaměstnanec firmy, může se jednat i o člověka vydávajícího se za jinou osobu nebo pohozenou disketu s lákavým názvem (např. s názvem "mzdy 2008"), která obsahuje zákeřný software. Tento software může následně zvědavý zaměstnanec zavést do firemní sítě.

Mezi další otázky bezpečnostní politiky firem patří celá řada zabezpečení. Zranitelná místa můžeme rozdělit na:

- Fyzická – výpadek sítě, vandalismus, sabotáž, …
- Přírodní – záplava, vítr, blesk, požár, …
- Fyzikální – útoky na datové cesty, …

Proto by se nemělo zapomínat na bezpečnostní politiku firem. Každá firma by si měla stanovit a sepsat bezpečnostní politiku a přeškolit své zaměstnance případně přímě i nepřímě spolupracovníky s firmou či systémem.

Hlavní faktory jak by měla být chráněna data[1], jsou tak:

- Aby k nim měly přístup pouze oprávněné osoby
- Aby se zpracovávaly nefalšované informace
- Aby se dalo zjistit, kdo je vytvořil, změnil nebo odstranil
- Aby nebyla nekontrolovaným způsobem vyzrazena
- Aby byla dostupná tehdy, když jsou potřebná.

Narušení bezpečnosti zpracování informací lze provést například[1]:

- Narušením soukromí či utajením informací
- Vydáváním se za jinou oprávněnou osobu a zneužíváním jejích privilegií

[112] Firewall – síťové zabezpečení provozu mezi sítěmi

- Distancováním se od odpovědnosti nebo od závazků plynoucích z manipulace s informací
- Tvrzením, že nějaká informace někam poslala a toto se nestalo
- Tvrzením, že se informace získala od nějakého podvodníka
- Neoprávněným zvýšením svých privilegií přístupu k informacím
- Modifikací privilegií ostatních osob
- Zatajením výskytu důvěrné informace v jiných informacích
- Zjišťováním, kdo a kdy si zpřístupňuje které informace
- Zařazením se jako skrytý mezičlánek v konverzaci jiných subjektů
- Pokažením funkcionality softwaru doplněním skrytých funkcí
- Narušením protokolu činností jiných subjektů zavedením nesprávných, nekorektních informací
- Podkopáním důvěryhodnosti protokolu způsobeným zjevným, byť možná jen zdánlivými poruchami
- Bráněním jiným uživatelům legitimně komunikovat.

Další informace o bezpečnostní politice firem v dokumentu “bezpečnost.pdf“ v příloze. Jedná se o metodickou příručku zabezpečování produktů a systémů budovaných na bázi informačních technologií.

3.5 Platby na internetu

V dnešní době mezi nejčastější platební způsoby za zboží a služby na internetu lze považovat platby pomocí platebních karet. Tato převaha plateb pomocí platebních karet se stále zmenšuje ve prospěch alternativních způsobů placení. V roce 2000 ve Spojených státech činil podíl platebních karet za platby 90%. Podle zprávy poradenské firmy Celent se celosvětově blíží doba, kdy alternativní způsoby platby začnou platební karty vytlačovat. V roce 2009 by mělo podle předpovědí být 26% pro alternativní platby. Informační zdroje z kterých jsem čerpal je web lupa.cz [41], bankovnictvi.ihnd.cz [42] a platba.cz [43].

Platební karta

Tento způsob plateb je nejvíce rozšířený. Pří platbě se do webového formuláře vepisují informace jako je jméno, číslo karty a datum platnosti. Případně je třeba dále vepsat CW2/CVC2[113] kód z karty pro vyšší bezpečnost.

Vrubopis

Obzvlášť jednoduchý způsob placení. Zákazník uděluje právo prodejci k tomu aby si mohl strnout splatné sumy z účtu zákazníka. Proti zneužití je tato metoda zabezpečená tak, že klient neoprávněně odečty peněz z účtu může během nějaké doby zablokovat. U prodejce nebo poskytovatele služeb může nastat problém z důvodu nedostatku peněz na účtu na straně klienta. Tento způsob plateb je rozšířený především v Německu. U vrubopisu je třeba dát pozor na znění obchodních podmínek.

Firstgate

Tento systém patří k nejlépe etablovaným alternativním platebním systémům na trhu. Po přihlášení u firstgate lze trvale platit na internetu u systémů, které jsou na tento systém napojené. Platba se provádí pomocí stisknutí jednoho tlačítka.

Paypal

Patří mezi celosvětově největší poskytovatele internetových plateb. Paypal patří internetovému aukčnímu domu eBay. Po registraci je možné posílat a přijímat peníze po celém světě. U paypal účtu je možné registrovat platební kartu nebo je nutné převést první peníze na tento paypal účet.

[113] CW2/CVC2 – kontrolní kód, CVC – Card Verification Code pro karty MasterCard, CW – karty VISA

Poplatku podléhá pouze připsání peněz na účet. Placení je zdarma. Platby mezi paypal účty při dostatku peněz na účtu probíhají okamžitě. Při platbě na jiný účet (třeba u nějaké banky) platba může trvat několik dní.

Platba na fakturu

V Evropě za služby a zboží na internetu se často nabízí platba na fakturu. Z hlediska zákazníka je to nejbezpečnější způsob placení. Potřebnou částku k úhradě převádí až po obdržení zboží na účet uvedený ve faktuře. U vystavitele faktury vzniká riziko, zda zákazník zaplatí a zda zaplatí včas.

Dialer

Dialer jsou malé prográmky, které připojují počítač na čísla služeb tzv. přidané hodnoty (například v Německu, 09009). U těchto čísel se počítají vyšší poplatky, které se poskytují částečně pro připojení a zbytek na dodatečné služby. Tyto prográmky zažívají útlum, za což může velká míra zneužití. V Německu tato technologie má stále velkou oblibu.

Prémiové SMS

Tato technologie na trhu je od roku 2002. Platební styk tzv. prémiové SMS si u nás dostává stále do větší obliby a stále tato technologie posiluje svůj podíl v alternativních platbách. Princip je, že zákazník posílá krátké sdělení pomocí SMS s heslem (heslo požadavku o co má zájem) na pětimístné telefonní číslo. Poplatky za odeslanou SMS jsou u těchto čísel mnohonásobné vyšší. Tímto poplatkem je hrazena požadována služba. Použití převážně pro menší částky.

Voice-call

Především na zábavních a erotických stránkách se vedle prográmků dialer používá také systém voice-call. Princip je jednoduchý, že zákazník zavolá na číslo s vysokým poplatkem. Za tento hovor zákazník dostává následně většinou heslo, které má omezenou platnost.

Platba mobilním telefonem nebo e-mailem

Mobilní a e-mailové platby se dostaly do podvědomí lidí v posledních letech. Dnes snad mezi tyto platby patří nejznámější PayPay nebo moneyBookers. MoneyBookers si u nás získal velkou oblibu, a je velice známý. V Česku pro tuto společnost existuje český účet, což zaručuje bezproblémový převod peněz. Koncem roku 2006 byl tento systém lokalizován do českého

jazyka. MoneyBookers je často a převážně spojováno se sazkovými kancelářemi. Dále bychom zde mohli zahrnou systémy jako je Fireplay nebo Neteller a podobně.

E-gold

Jedná se o platební systém, při němž se u mezinárodních transakcí účtuje ve zlatě. Po vytvoření účtu je možné pomocí platební karty nebo převodu z účtu nakoupit požadované množství zlata a poté toto zlato převádět na další uživatele nebo platit s ním. Roční poplatky jsou v rozsahu 1% vlastněného zlata. Tento systém má přes 3milióny uživatelů po celém světě.

Srovnání plateb na internetu

Tabulka zobrazuje přehled jednotlivých plateb a jejich výhody a nevýhody:

Druh platby	Výhody	Nevýhody
platební karta	jednoduché placení, široce rozšířené, velice spolehlivé	možnost zneužití údajů z platební karty
vrubopis	téměř žádné riziko zneužití	nutný podpis na zmocnění obchodníka k inkasu peněz => styk s poštou nebo nutno faxovat, pro malé platby nevhodné
Firstgate	bezpečné, po přihlášení nekomplikované, i pro malé platby, mnohostranný systém	nutné přihlášení, poplatky pro firstgate
Paypal	celosvětové použití, bezpečný převod, vhodné pro účast na eBay aukcích, rychlá platba mezi paypal účty	poplatky, plné využití jen pro majitele platební karty, platby mimo účty paypal trvají dlouho
platba na fakturu	nejvíce bezpečné	nevhodné pro malé částky, bankovní převod
dialer	jednoduché používání, vhodné pro malé částky	netransparentnost, neseriozní obchodník, vysoké a nepřehledné ceny,
prémiové SMS	rychlé a jednoduché použití	nedostatečně transparentní, prodejce těžko identifikovatelný,obchodní podmínky většinou špatně přístupné
voice-call	snadno použitelné	cenová struktura není vždy transparentní
platba mobilním telefonem nebo e-mailem	rychlost a snadná použitelnost	nutné přihlášení, poplatky
e-gold	Možnost převodu po celém světě, anonymní	složité vedení konta

Tabulka 10: Srovnání plateb na internetu

4 Zadání

Zadání diplomové práce je na téma: Systém pro evidenci personální a mzdové agendy. Pro tvorbu tohoto systému byla zapotřebí konzultace se mzdovou účetní a prozkoumání dostupných programů pro mzdovou a personální evidenci. V důsledku toho byly zvolené vstupní požadavky na řešení.

4.1 Požadavky na řešení

Funkce informačního systému:

- Informace o provozující společnosti
- Firemní agenda
  - Správa registrovaných firem – výběr evidované firmy
  - Prohlížení / zadávání / editace / tisk firemních údajů (firemní údaje, adresy, kontakty, bankovní spojení, kalendáře, střediska)
  - Prohlížení / zadávání / editace / tisk zakázek pro firmu
  - Registrace uživatelů k firmě
- Personální agenda
  - Prohlížení / zadávání / editace / tisk / vyhledávání zaměstnanců (osobní údaje, adresy, kontakty, bankovní spojení, znalosti, školení, zdravotní stav)
  - Prohlížení / zadávání / editace / tisk / vyhledávání dětí zaměstnanců
  - Evidování pracovních poměrů – mzdové údaje
- Mzdová agenda
  - Prohlížení / zadávání / editace / tisk / vyhledávání mzdových údajů (mzdové údaje, slevy na dani, prémie, naturální mzda, srážky, exekuce, příspěvky)
  - Prohlížení / zadávání / editace šablon pracovního plánu (šablona pracovního plánu, příplatky)
  - Evidování pracovních poměrů – mzdové údaje
  - Modul pro vkládání úkolových listů
  - Prohlížení / zadávání / editace úkolového listu pro osobu
  - Uzavření úkolového listu
  - Zadávání odpracováno (vázáno na zakázky firmy), nemoc, dovolená, omluvená a neomluvená absence a překážka v práci
  - Probarvení víkendu a svátku (dle kalendáře firmy)
  - Hromadná změna stavu

        - Přenos pracovního dne na výběr dalších dnů
        - Přenesení úkolového listu na jiného zaměstnance a pracovní poměr
        - Sekce s rolí mistr pro zadávání úkolového listu
        - Modul výpočet mezd
        - Prohlížení / zadávání / editace / tisk výplatního listu
        - Načtení úkolového listu do výpočtů mezd z možnosti úprav přenesených hodnot
        - Načtení hodnot ze mzdového údaje
        - Výpočet náhrady mzdy na nemoc
        - Srážky ze mzdy
        - Výpočet mezd dle typu mzdy
        - Roční zúčtovaní daně, jednoduché daňové přiznání
    - Tiskové sestavy
    - Modul s podporou bankovních příkazů
    - Měsíční výkazy pro mzdy
        - Sociálka – pro danou firmu
        - Zdravotní poj. – pro zaměstnance
        - Výkaz daně – pro zaměstnance (výkaz jako celek pro celou firmu)
    - Správa systému
        - Přihlášení do systému
        - Změna hesla
        - Nápověda
        - Help Desk[114] v oblasti informačního systému
        - Správa číselníků
        - Správa uživatelů – firem
        - Správa rolí
        - Statistiky
        - Změna témat vzhledu

Další požadavky na tvorbu informačního systému:

- Realizace prezentace informačního systému
- Lokalizace jazykového prostředí
- Možnost změny grafického návrhu – změna CSS[115] stylu
- Možnosti rozšíření systému

[114] Help Desk – v IT jde o poskytnutí technické podpory uživatelům PC či jiných zařízení
[115] CSS – Cascading Style Sheets – kaskádové styly pro návrh webových stránek

- Návrh zabezpečení
- Nezávislé výstupy – použití PDF[116] formátu

4.2 Stanovení cíle diplomové práce

Tato diplomová práce si klade za cíl provést teoretický rozbor mzdové problematiky pro tvorbu informačního systému pro mzdovou a personální agendu. Dále se také diplomová práce snaží provést rozbor problematiky bezpečnosti informačního systému hlavně z pohledu autentizace, autorizace a srovnání plateb na internetu. Na základě požadavku se tato práce snaží vytvořit univerzální analýzu, návrh a implementaci informačního systému v prostředí .NET[117].

Je kladen důraz na:

- Teoretický základ k problematice mzdové a personální agendy
- Teoretický základ k problematice výpočtů mezd
- Teoretický základ k problematice bezpečnosti informačních technologií
- Problematika metod pro autentizaci
- Problematika plateb na internetu
- Nezávislý datový návrh jádra informačního systému
- Implementace informačního systému v prostředí .NET pro běh na internetu
- Tvorba nezávislých výstupních sestav na prostředí a typu internetového prohlížeče
- Tvorba uživatelské a programátorské příručky

[116] PDF – Portable Document Format – přenosný formát dokumentů – souborový formát vyvinutý firmou Adobe pro ukládání dokumentů nezávisle na softwaru i hardwaru

[117] .NET – .NET Framework firmy Microsoft

5 Analýza

5.1 Datová analýza

Základním prvkem pro tvorbu informačního systému je datová analýza [1]. Před návrhem datové analýzy bylo důležité se seznámit s možností a vlastnostmi informačních systémů pro personální a mzdovou agendu. Základem bylo nutné projít určitou množinu programů (demoverze[118] i plnohodnotné verze) pro personální a mzdovou agendu. Na základě srovnání potřeb evidovaných položek různých programů a na základě konzultací se mzdovou účetní byly stanoveny podmínky pro datovou analýzu. Pro návrh je nutné taky pochopit základy pro výpočet mezd a další množinu informací pro mzdové účetnictví. Následně jsem musel nedefinovat stavy, ve kterých se systém může nacházet.

Dále jsem se snažil do systému zahrnout logiku, kterou jsem jinde neviděl. Ta se zaměřuje hlavně na vylepšení úkolového listu a jeho vyplňování pro zaměstnance. Dalším vylepšením, s kterým se muselo počítat při datové analýze je vytvoření pracovního plánu a šablon pracovního plánu. To by mělo usnadnit vytváření pracovních poměrů a vyplňování dat. Firma si vytvoří šablony pracovního plánu, které bude moci přiřazovat zaměstnancům do pracovního plánu. Využití je pro zaměstnance, kterých je víc než jeden stejného profilu práce. Pro pozici ředitele už se taková výhoda ztrácí, ale nenavyšuje žádnou režii pro zadávání. Pracovní plán by měl kromě základných údajů o pracovní pozici, platu, pracovní době a režimu, druhu činnosti apod. také obsahovat údaje o příplatcích a odměnách. Zaměstnanec má pak pracovní plán, kde má šablonu pracovního plánu a další údaje už jenom k jeho osobě jako např. středisko, odpracováno hodin, prémie, naturální mzdu, atd.

Při návrhu nelze zapomenout na legislativu České republiky, tedy zákon č. 85/2001 Sb. zákoník práce a případně další zákony např. zákon o mzdě, zákon o platu a pod., které se zabývají pracovním právem[119]. Do systému je taky potřeba zabudovat řadu bezpečnostních opatření, která jsou v dnešní době kladena na bezpečný IS[120].

Při datové analýze byl kladen důraz na obecné provedení, tedy je možné systém implementovat v libovolném prostředí programovacího jazyka. Datové úložiště pro systém je zvolená relační databáze. Do datové analýzy byla snaha zahrnout co nejvíce možností pro předpokládané možné změny v legislativě ČR[121] a tedy změny i v systému. To by mělo zabránit větším zásahům do

[118] Z ang. slova demo v překladu demonstrační, předváděcí program
[119] Zákony např. na: http://zakony-online.cz/
[120] IS – informační systém
[121] ČR – Česká Republika

systému. Bohužel neočekávaným změnám se nevyhneme a musíme počítat s pozdějšími update[122] celého systému.

Na základě dat shromážděných pro potřeby systému pro mzdovou a personální agendu byla snaha o navrhnutí datového schématu databáze ve 3. normální formě. Návrh databáze tuto formu nesplňuje a snaží se ji co nejvíce přiblížit. Z důvodu rychlosti systému nebo zjednodušení implementace systému bylo v určitých částech návrhu poleveno z nároku na 3. normální formu. Nejvíce duplicita dat lze vidět u tabulek WorkSheet, WorkSheetSum a Wages. Aby nedocházelo k opakovatelnému počítání hodnot a zpomalování systému, je tabulka WorkSheetSum součtovou tabulkou pro tabulku WorkSheet.

Do datové analýzy se už postupně proplétaly možnosti uživatelského rozhraní, tedy uskupení jednotlivých tabulek a dat podle budoucího uživatelského rozhraní. Aby bylo možné udělat uživateli formuláře co možná nejvíce intuitivní, bylo nutné v analýze s tím počítat. Pozdější změny a optimalizace dat by měly za následek změnu datové analýzy a celkovou iterací ve vývoji informačního systému. Při tomto prolínání datové analýzy a analýzy návrhu se nesmělo zapomenout na nezávislost na libovolném programovacím a datovém prostředí.

Pro tvorbu tabulek byla zvolena následující konvence:

- Názvy tabulek začínají velkým písmenem
- Pokud název tabulek má více slov, každé další slovo začíná velkým písmenem bez mezery
- Názvy vazebních tabulek začínají prefixem “R_“
- Primární a sekundární klíče obsahují prefix “id_“ a následně obsahují tři písmena z názvu tabulky např. “id_per“ (pokud název už neexistuje, případně podtržítko a další tři písmena např. “id_ban_con“)
- Atributy obsahují pouze malé písmena
- Pokud se atribut skládá s více slov, další slovo začíná malým písmenem za podtržítkem např: “next_first_name“

5.1.1 E-R diagram[123]

Návrh datové analýzy je velmi rozsáhlý a tedy i datová struktura E-R diagram. Pro velkou rozsáhlost se mi nepodařil E-R diagram umístit na jednu stránku. S tohoto důvodu byl E-R diagram rozdělen na několik stránek. Pro rozdělení jsem si zvolil několik hlavních tabulek a to tabulky: Company, BankConnection, Person a WagesData. Tyto tabulky na různých stránkách

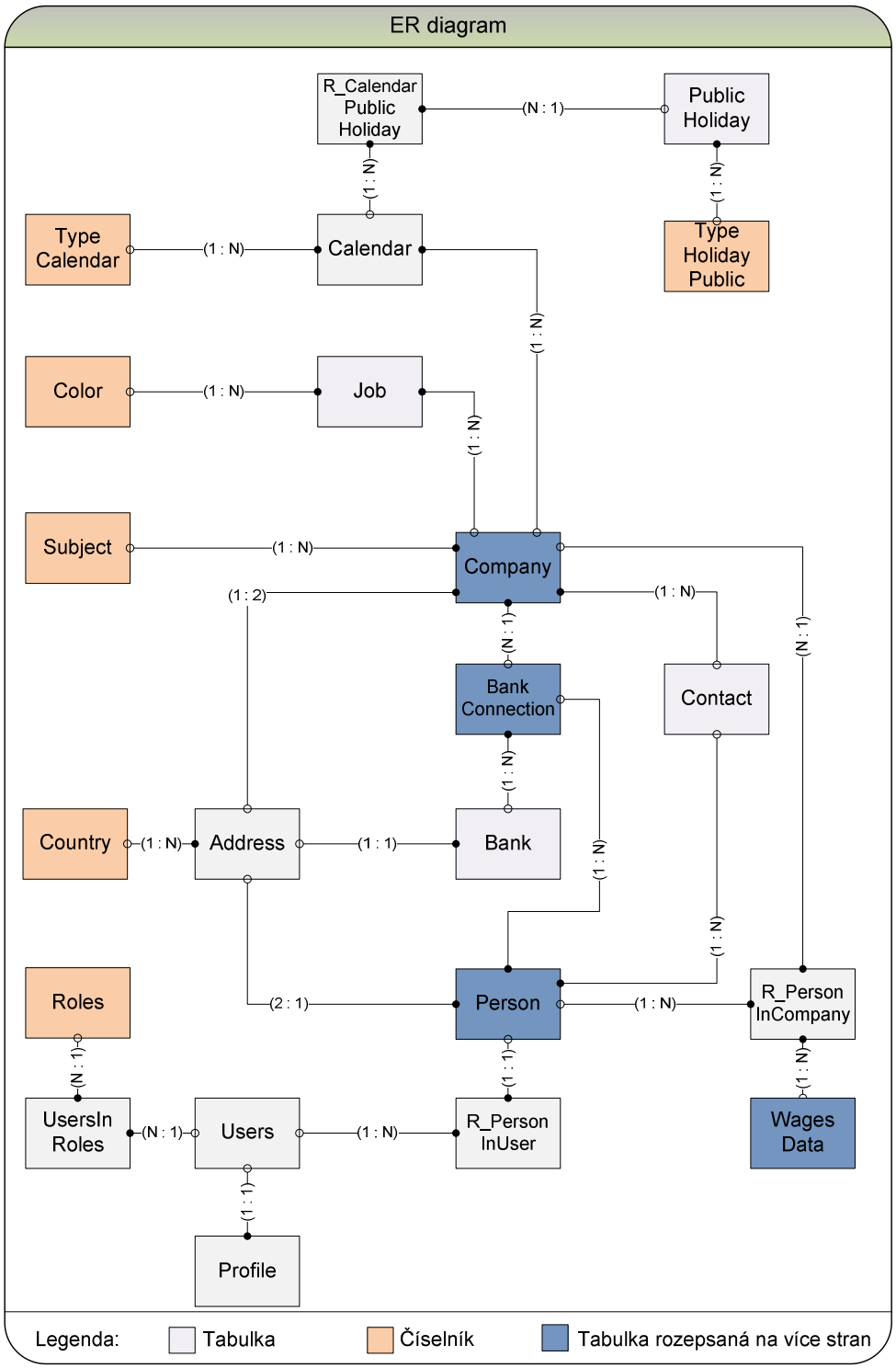
[122] Z ang. slova update v překladu aktualizovat, zmodernizovat

[123] E-R diagram – Entity – relationship model

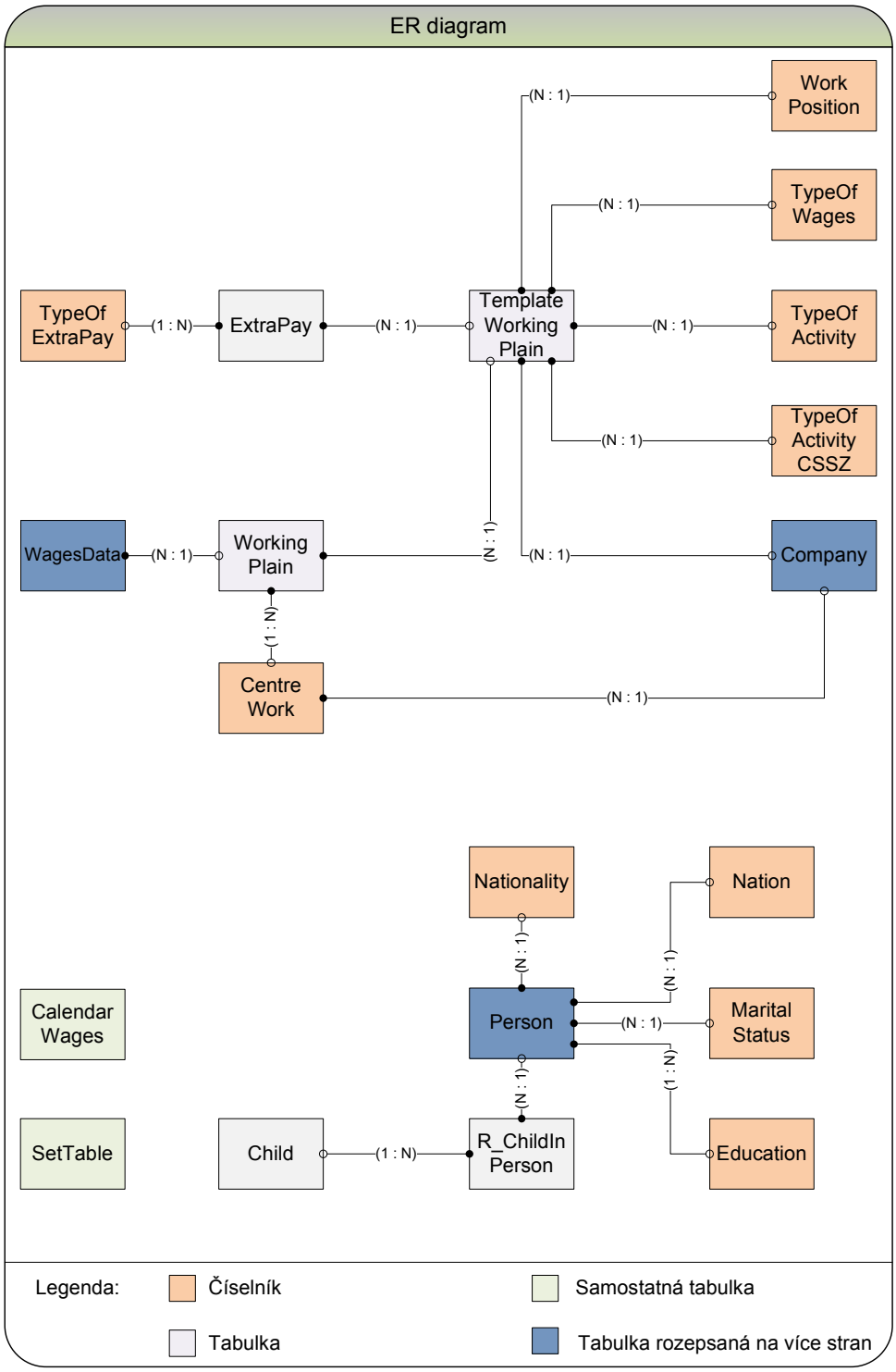
jsou identické. Tabulky jsou taky barevně označené pro jejich význam v databázi. Barevné označení slouží pro rychlejší orientaci a pro zpřehlednění E-R diagramu běžnému uživateli. Názvy tabulek jsou stejně jako v databázi v anglickém jazyce. Návrh (později i implementace) je v anglickém jazyce, aby případně i člověk neznající český jazyk se dovedl zorientovat v datové analýze. Lokalizaci[124] E-R diagramu do českého jazyka najdete na přiloženém CD[125] v příloze. E-R diagram kromě barevného rozlišení tabulek a jejích názvu obsahuje vazby s povinnostmi a kardinalitou. E-R diagram už neobsahuje vazby N:M.

[124] Přeložení

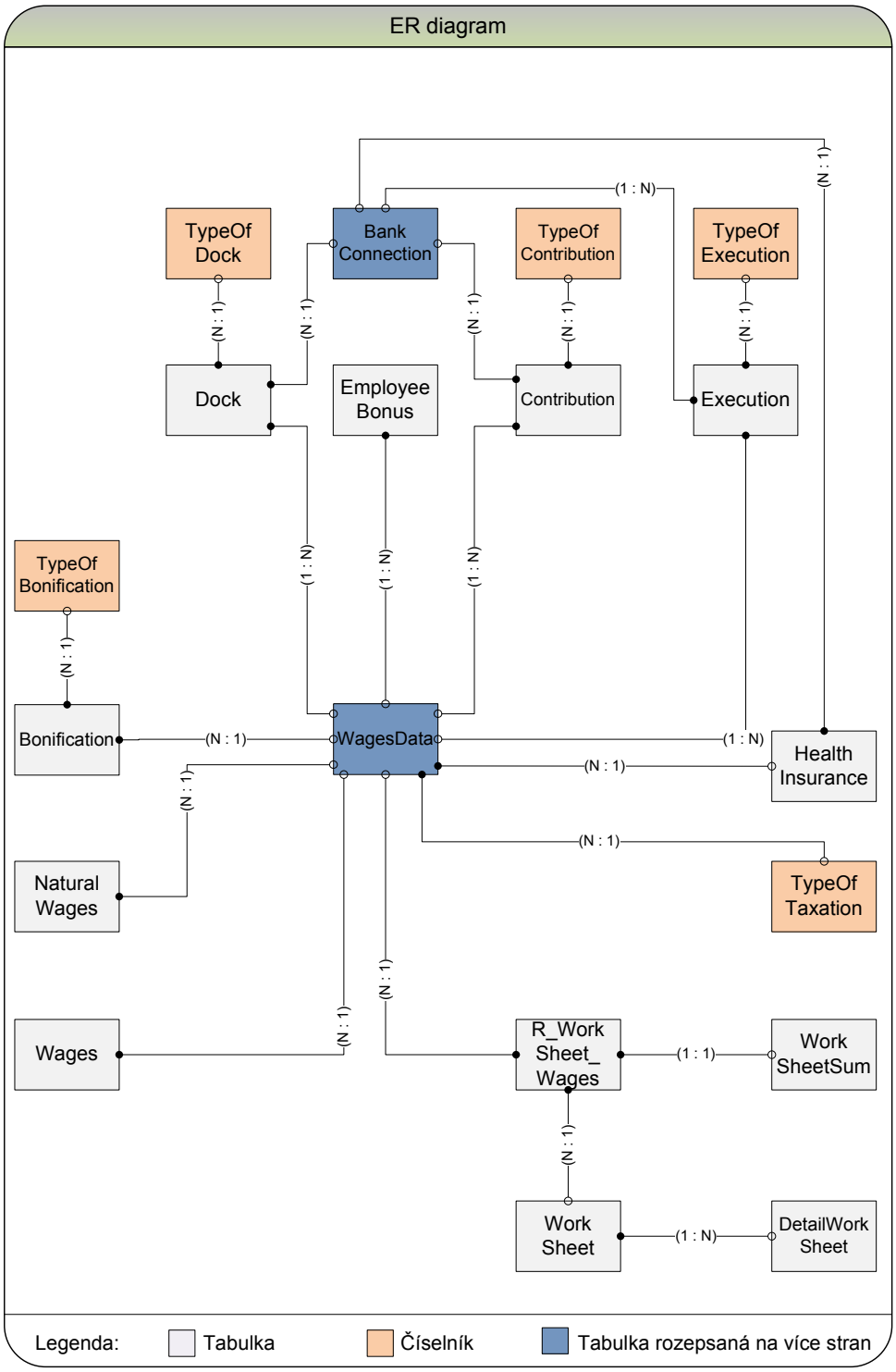
[125], [12] CD - Compact disk – zálohovací medium



Obrázek 7: E-R diagram – část 1



Obrázek 8: E-R diagram - část 2



Obrázek 9: E-R diagram - část 3

5.1.2 Datový slovník

V datovém slovníku jsou názvy tabulek odvozené z E-R diagramu. Názvy tabulek a jednotlivých atributů pro tabulky jsou v českém i anglickém jazyce. Implementace v databázi je provedena celkově v anglickém jazyce. Datový slovník je rozsáhlý a z tohoto důvodu je umístěn na přiloženém CD v příloze.

Seznam implementovaných tabulek:

- Address - tabulka objektů adres na osobu/firmu
- AverageHourPay - tabulka objektů průměrných výdělků pro zaměstnance
- Bank - tabulka objektů bank
- BankConnection - tabulka objektů bankovních spojení
- Bonification - tabulka slev na dani
- Calendar - vazební tabulka mezi kalendářem a firmou
- CalendarWages - tabulka obsahující pracovní kalendář
- CentreWork - číselník pracovních středisek
- Color - číselník barev pro zakázky
- Company - tabulka objektů obsahující firmy
- Contact - tabulka objektů kontaktů na osobu/firmu
- Contribution - tabulka objektů finančních příspěvků
- Country - číselník státu
- DetailWorkShet - tabulka objektů odpracovaných hodin k zakázce
- Dock - tabulka objektů srážek ze mzdy
- Education - číselník vzdělání
- EmployeeBonus - tabulka objektů s prémiemi zaměstnanců
- Execution - tabulka objektů exekuce
- ExtraPay - tabulka příplatků
- HealthInsurance - tabulka zdravotních pojišťoven
- Child - tabulka objektů obsahující dětí
- Job - tabulka objektů obsahující zakázky
- MaritalStatus - číselník rodinného stavu

- MeritBonus - tabulka odměn za dobrou práci
- Nation - číselník národnosti
- Nationality - číselník státní příslušnosti
- NaturalWages - tabulka objektů obsahující naturální mzdu
- Person - tabulka objektů osob – osobní údaje
- Profile - tabulka obsahující hodnoty profilu uživatele IS
- PublicHoliday - tabulka obsahující svátky
- R_CalendarPublicHoliday - vazební tabulka mezi kalendářem a svátkem
- R_ChildInPerson - vazební tabulka mezi osobou a dítětem
- R_PersonInCompany - vazební tabulka mezi osobou a firmou
- R_PersonInUser - vazební tabulka mezi osobou a uživatelským jménem
- R_WagesData_Wages - vazební tabulka mezi mzdový údaj a výpočet mzdy
- R_WorkSheet_Wages - vazební tabulka mezi mzdový údaj a úkolový list
- Roles - tabulka obsahující role
- SetTable - tabulka obsahující základní nastavení systému
- Subject - číselník typu subjektů pro firmu
- TemplateWorkingPlan - tabulka objektu šablon pracovního plánu
- TypeCalendar - číselník typu kalendáře
- TypeHolidayPublic - typ svátku
- TypeOfActivity - číselník druhu činnosti pro mzdový údaj
- TypeOfActivityCSSZ - číselník druhu činnosti pro CSSZ
- TypeOfBonification - číselník slev na dani
- TypeOfContribution - číselník typu finančního příspěvku
- TypeOfDock - číselník typu srážky ze mzdy
- TypeOfExecution - číselník typu exekucí
- TypeOfExtraPay - číselník typu příplatků
- TypeOfTaxation - číselník typu zdanění
- TypeOfWages - číselník typu mzdy

- UserInRoles - vazební tabulka mezi uživatelem a roli
- Users - tabulka uživatelů IS
- Wages - tabulka objektů mezd
- WagesData - tabulka objektů mzdových údajů
- WorkingPlain - tabulka objektů pracovních plánů
- WorkPosition - číselník typu pracovní pozice
- WorkSheet - tabulka objektu úkolový list
- WorkSheetSum - tabulka obsahující součty úkolového listu

Pro nezávislý návrh datové analýzy byli použité zkratky v datovém slovníku označující datové typy. Tyhle zkratky nepředstavují vazby na žádnou databázovou platformu. Délka v datovém slovníku představuje počet písmen u textových položek a počet číslic u číselných položek. Každá položka v datovém slovníku může být ještě následně omezená integritním omezením.

Seznam zkratek použitých v datovém slovníku:

- Numeric - celočíselná kladná hodnota – celočíselné číslo
- Character - textová položka – jedná se o kombinaci znaků, čísel a speciálních symbolů
- Date - jedná se o datovou položku. Datum se ukládá ve tvaru datum + čas. Tedy DD.MM.RRRR HH.MM.SS.
- Bool - jedná se o logickou hodnotu. Tato hodnota může být definována jako výčtový typ o dvou stavech. V závislosti na použití databázového prostředí může být použita hodnota integer o délce 1 s hodnotami 1 a 0. Nebo může být použít datový typ bit.
- double - hodnota s desetinnou čárkou. Pokud je číselná hodnota označena hodnotou např. “3,2“ znamená to, že číselná hodnota obsahuje tři čísla před desetinnou čárku a dvě čísla za desetinnou čárku.

5.2 Funkční analýza

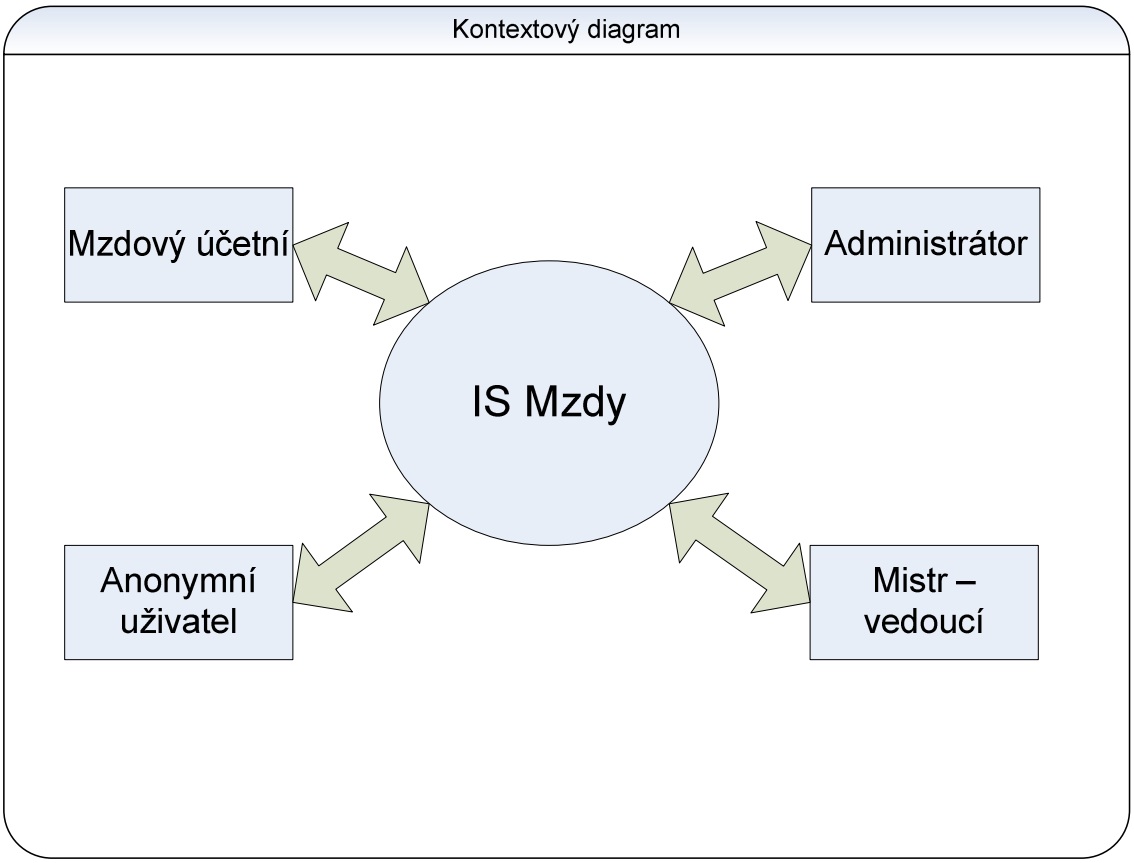
Ve vývoji tohoto informačního systému je dalším krokem funkční analýza, která navazuje na datovou analýzu. Dalším vstupem do funkční analýzy je seznam funkcí požadovaných od systému. Tato analýza popisuje dané funkce, jejích chování v systému, datové úložiště a jejich

výstupy. Funkční analýza nám poskytuje kontrolní pohled na vytvářený informační systém. Máme zde grafické znázornění funkcí propojitelné s datovým modelem. Tyto DFD[126] diagramy jsou hierarchické. Pro nedostatek času nejsou rozepsané veškeré DFD diagramy. Vybral jsem pro znázornění jen několik složitějších DFD diagramů.

V DFD analýze se vyskytují aktéři (uživatelé systému nebo jiné systémy), datové sklady (uchovává data), procesy (manipulují s daty) a datové toky.

5.2.1 Kontextový diagram

Kontextový diagram nám poskytuje pohled na celý informační systém a zobrazuje aktéry, kteří pracují s informačním systémem.



Obrázek 10: Kontextový diagram

Do informačního systému "IS Mzdy" vstupují čtyři skupiny uživatelů:

[126] DFD – Data Flow Diagram – představují chování funkcí z hlediska datových toků

- Anonymní uživatel — běžný uživatel přicházející na webové stránky informačního systému – nemá žádná přístupová práva do chráněných částí
- Mistr — uživatel, který má práva vyplňovat úkolové listy zaměstnanců dané firmy
- Mzdový účetní — uživatel s oprávněným zadáváním údajů do systému
- Administrátor — správce informačního systému

5.3 Seznam funkcí

Seznam funkcí vznikl na základě požadavku na informační systém. Tento seznam by měl pokrývat veškeré požadavky na základní chování informačního systému. Jedná se o první iteraci vývoje IS, proto v dalších iteracích můžou být doplněné další funkce pro zkvalitnění systému. Jednotlivé funkcionality jsou rozdělené do skupin. Jedná se o hierarchickou strukturu zpodrobňování jejích jednotlivých akcí.

1. **uživatelé**
   - **1.1. anonymní uživatel**
     - 1.1.1. přihlášení
     - 1.1.2. zobraz dokument (8.3.1.)
     - 1.1.3. zobraz jak na to (8.4.1.)
   - **1.2. mistr**
     - 1.2.1. anonymní uživatel (1.1.)
     - 1.2.2. úkolový list (5.)
   - **1.3. mzdový účetní**
     - 1.3.1. změn účtovanou firmu
     - 1.3.2. mistr (1.2.)
     - 1.3.3. nastavení (heslo, téma vzhledu, atd.)
     - 1.3.4. firemní agenda (2.)
     - 1.3.5. personální agenda (3.)
     - 1.3.6. mzdová agenda (4.)
     - 1.3.7. mzdy (7.)
     - 1.3.8. tisk (5.)
   - **1.4. administrátor**
     - 1.4.1. mzdový účetní (1.3.)
     - 1.4.2. údržba (8.)
2. **firemní agenda**
   - 2.1. vyhledej firmu

2.2. prohlížej firmu

2.2.1. správa zakázek

2.2.1.1. vyhledej zakázku

2.2.1.2. vlož zakázku

2.2.1.3. edituj zakázku

2.2.1.4. zablokuj zakázku

2.2.2. správa firemních kalendářů

2.3. vlož firmu

2.4. edituj firmu

2.5. tisk

2.6. fakturace

2.6.1. vyhledej fakturu

2.6.2. edituj fakturu

2.6.3. platba

2.6.4. tisk

3. personální agenda

3.1. vyhledej osobu

3.2. prohlížej osobu

3.2.1. správa dětí

3.2.1.1. vyhledej dítě

3.2.1.2. vlož dítě

3.2.1.3. edituj dítě

3.2.1.4. tisk

3.3. vlož osobu

3.4. edituj osobu

3.5. tisk

4. mzdová agenda

4.1. vyhledej osobu (3.1.)

4.1.1. vyhledej mzdový údaj pro osobu

4.1.2. vyber mzdový údaj

4.1.3. prohlížej mzdový údaj

4.1.3.1. vyhledej slevy na dani

4.1.3.2. vlož slevu na dani

4.1.3.3. edituj slevu a dani

4.1.3.4. vyhledej prémie

4.1.3.5. vlož prémii

4.1.3.6. edituj prémii

4.1.3.7. vyhledej naturální mzdy

4.1.3.8. vlož naturální mzdu

4.1.3.9. edituj naturální mzdu

4.1.3.10. vyhledej srážky
4.1.3.11. vlož srážku ze mzdy
4.1.3.12. edituj srážku ze mzdy
4.1.3.13. zablokuj srážku ze mzdy
4.1.3.14. vyhledej exekuce
4.1.3.15. vlož exekuci
4.1.3.16. edituj exekuci
4.1.3.17. zablokuj exekuci
4.1.3.18. vyhledej příspěvky
4.1.3.19. edituj příspěvek
4.1.3.20. vlož příspěvek
4.1.3.21. zablokuj příspěvek
4.1.4. edituj mzdový údaj
4.1.5. úkolový list (6.)
4.1.6. mzdy (7.)

4.2. šablona pracovního plánu

4.2.1. vyhledej šablonu pracovního plánu

4.2.2. prohlížej šablonu pracovního plánu

4.2.2.1. vyhledej příplatek
4.2.2.2. prohlížej příplatek
4.2.2.3. vlož příplatek
4.2.2.4. edituj příplatek

4.2.3. vlož šablonu pracovního plánu
4.2.4. edituj šablonu pracovního plánu

4.3. střediska

4.3.1. vyhledej středisko
4.3.2. vlož středisko
4.3.3. edituj středisko

5. tisk

5.1. seznam zaměstnanců – jednoduchý
5.2. seznam zaměstnanců – podrobný
5.3. detail zaměstnance
5.4. detail dítěte
5.5. seznam firem – jednoduchý
5.6. seznam firem – podrobný
5.7. detail firmy
5.8. seznam zakázek
5.9. výplatní list
5.10. rekapitulace mezd – sociální pojištění
5.11. přehled o výši pojistného a vyplacených dávkách

5.12. rekapitulace mezd – výplaty
5.13. přehled pro zdravotní pojišťovny
5.14. mzdový list
5.15. potvrzení o zdanitelných příjmech

6. úkolový list

6.1. edituj úkolový list
6.1.1. načti úkolový list
6.1.2. správa úkolového listu (6.3.)

6.2. nový úkolový list
6.2.1. správa úkolového listu (6.3.)

6.3. správa úkolového listu
6.3.1. převést úkolový list
6.3.2. změn stav
6.3.3. ulož/edit úkolový list
6.3.4. přenést den
6.3.5. reset dne
6.3.6. uzavřít úkolový list

7. mzdy

7.1. edituj mzdu
7.1.1. správa mzdy (7.3.)

7.2. nová mzda
7.2.1. správa mzdy (7.3.)

7.3. správa mzdy
7.3.1. načíst úkolový list
7.3.2. výpočet mzdového listu
7.3.2.1. výpočet náhrady mzdy za nemoc
7.3.3. uzavřít mzdu
7.3.4. tisk mzdy
7.3.5. Načíst mzdové údaje
7.3.6. Ulož mzdu

8. údržba

8.1. vyhledej uživatele
8.2. změna hesla uživateli

8.3. správa rolí
8.3.1. zobraz role
8.3.2. přidej uživateli roli
8.3.3. smazej uživateli roli

8.4. statistika uživatele

8.5. číselníky
8.5.1. správa státu

8.5.2. správa bank
8.5.3. správa slev na dani
8.5.4. správa srážek
8.5.5. správa příspěvku
8.5.6. správa exekucí
8.5.7. správa pracovních pozic
8.5.8. správa zdravotních pojišťoven
8.5.9. správa plánovacího kalendáře

8.6. nastavení

8.6.1. změna hesla
8.6.2. změna vhledu IS

8.7. jak na to

8.7.1. zobraz jak na to
8.7.2. přidej jak na to
8.7.3. edituj jak na to
8.7.4. smaž jak na to

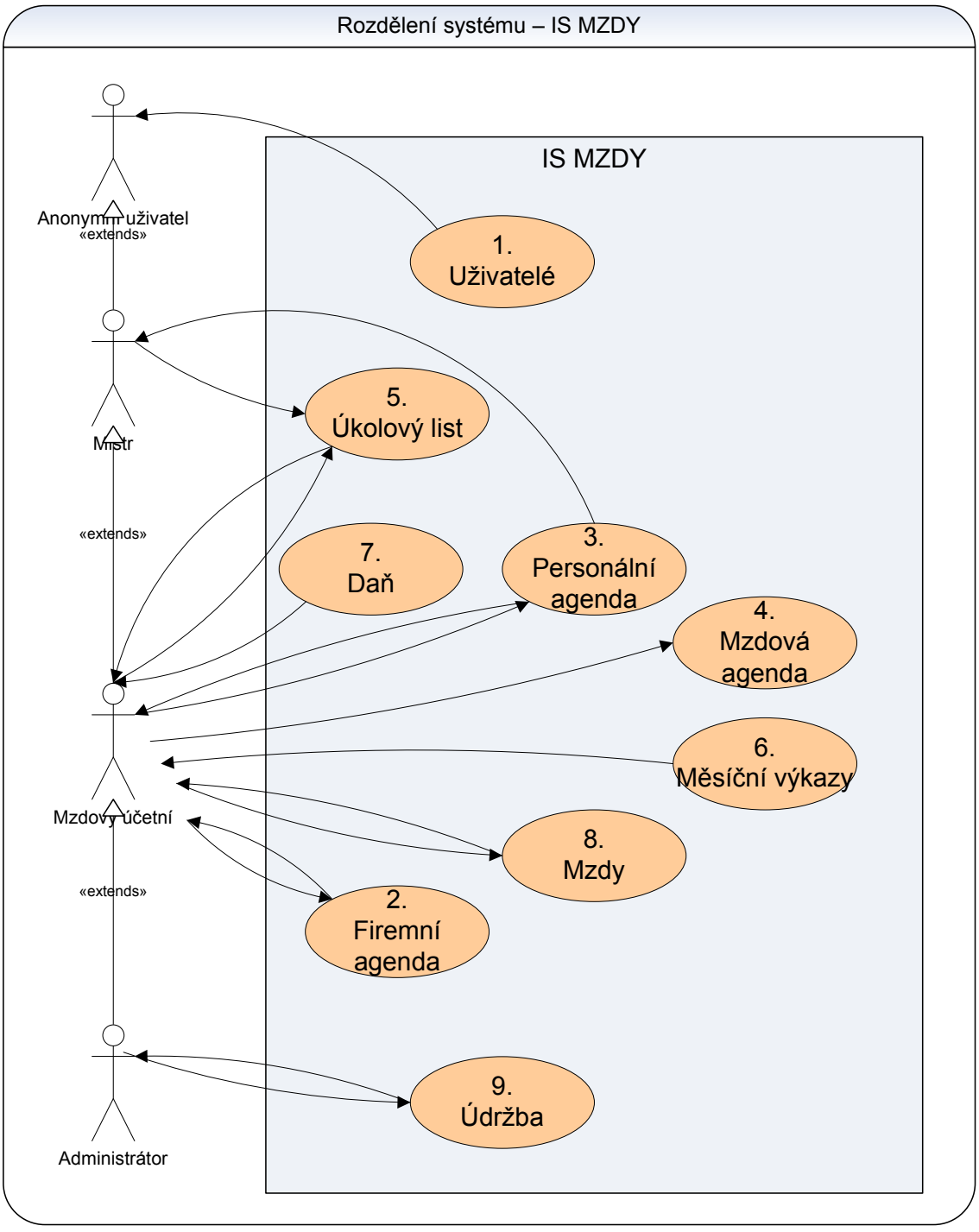
8.8. údržba systému

8.8.1. údržba tabulek
8.8.2. mazaní nepotřebných dat
8.8.3. log soubor

5.4 DFD diagramy

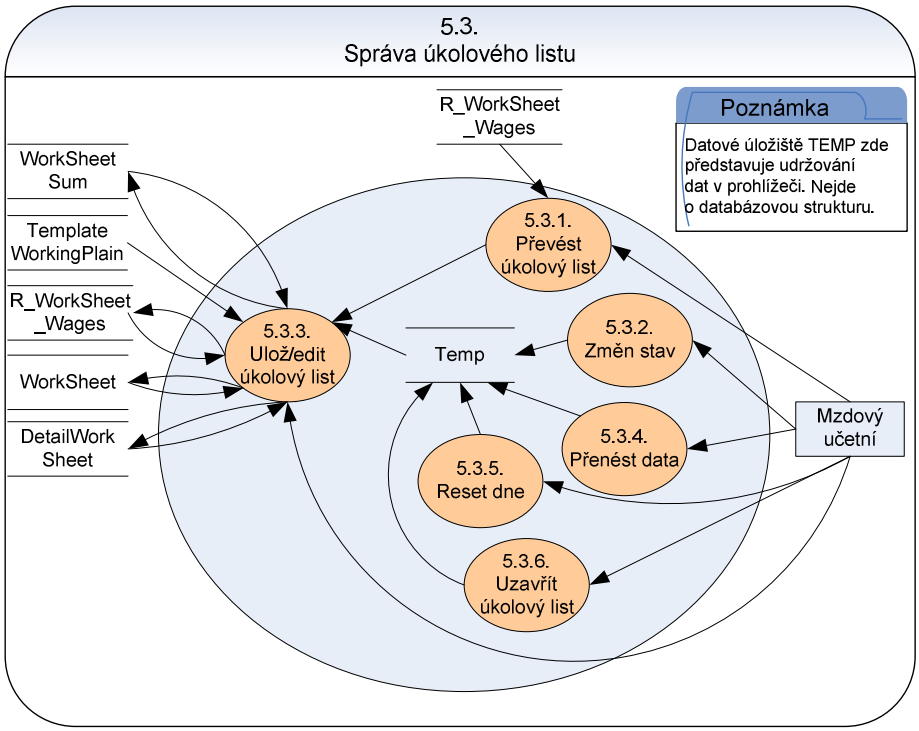
DFD[127] diagramy představují chování funkcí z hlediska datových toků. První DFD diagram nultého stupně je poupravený. Zobrazuje vztah uživatelů k systému. Nacházejí se zde uživatelé, kteří mají naznačenou hierarchickou dědičnost. K tomuto kroku jsem dospěl pro zjednodušení a přehlednost DFD diagramu nulté úrovně.

[127] DFD – Data Flow Diagram

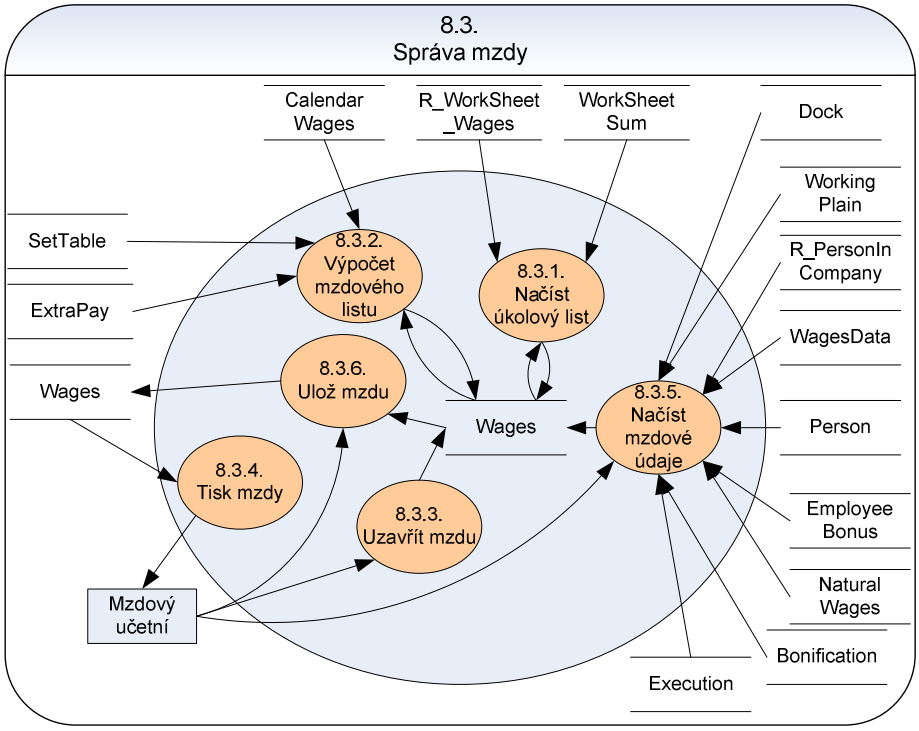


Obrázek 11: DFD nulté úrovně: rozvržení systém

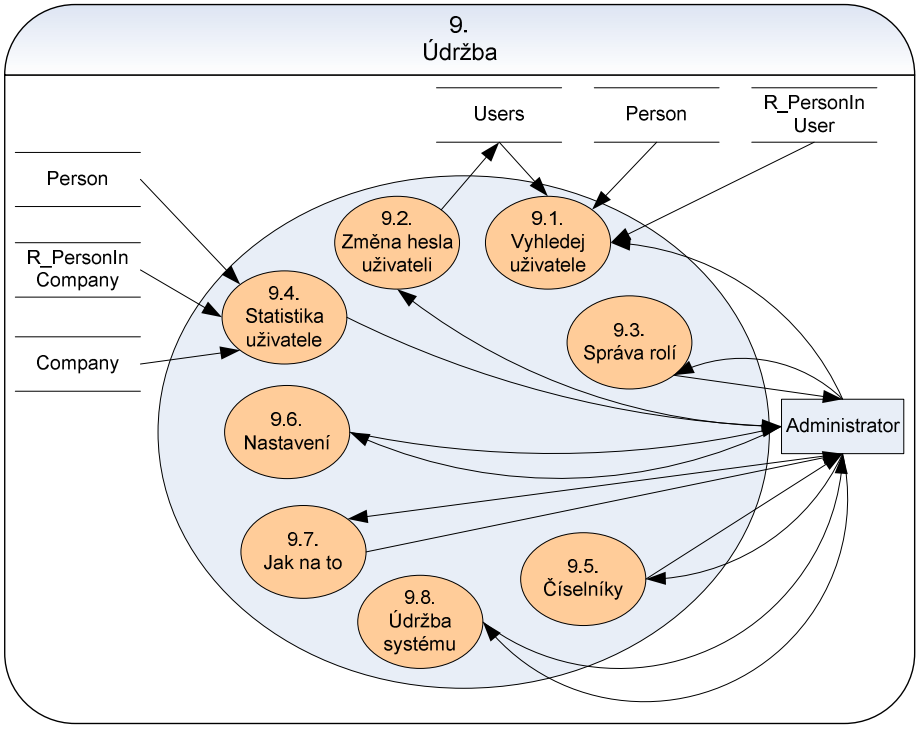
Dále zde je zobrazeno několik DFD diagramů pro ukázku.



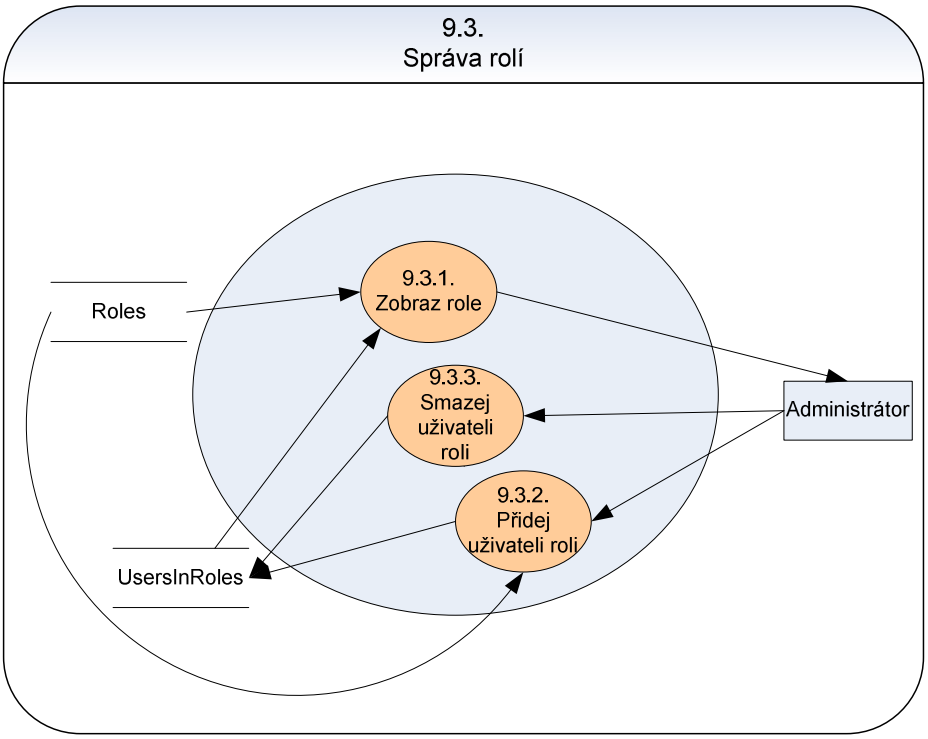
Obrázek 12: DFD 5.3. Správa úkolového listu



Obrázek 13: DFD 8.3. Správa mzdy



Obrázek 14: DFD 9. Údržba

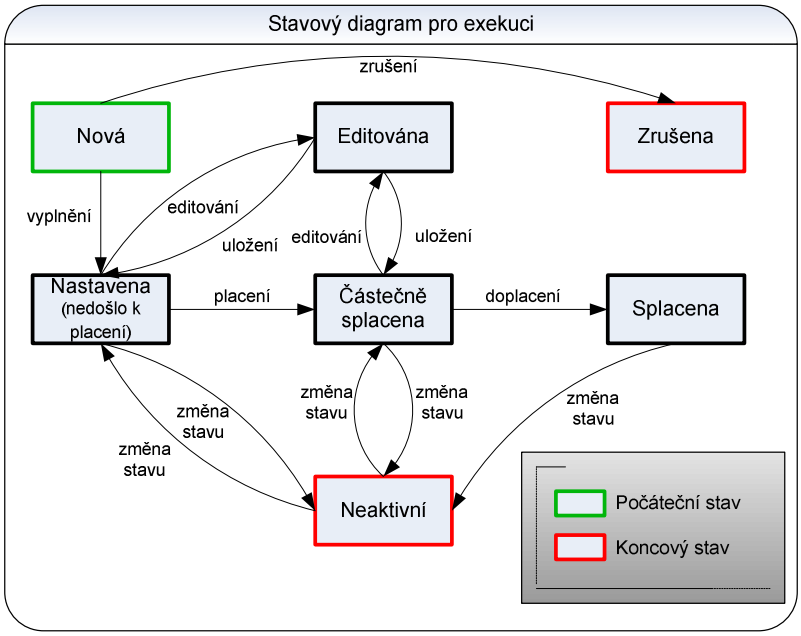


Obrázek 15:DFD 9.3. Správa rolí

5.5 Stavové diagramy

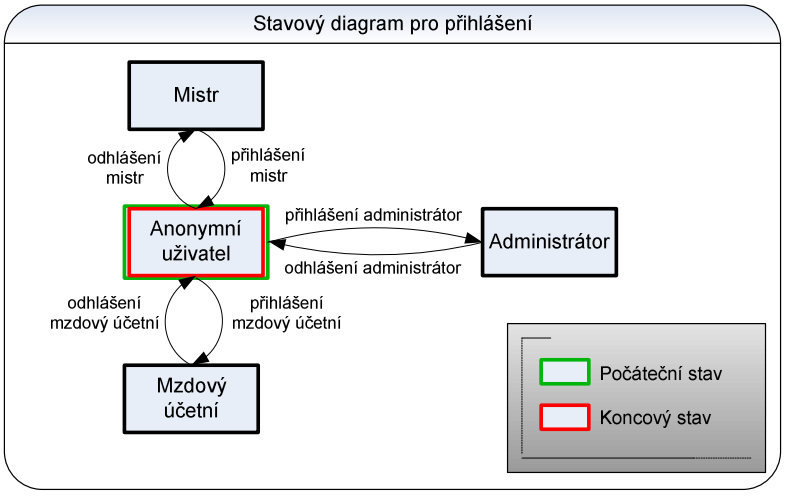
Časová analýza je řešena pomocí stavových diagramů. Tyto diagramy nám popisují stavy chování. Jednotlivé části systému nebo objekty se mohou nacházet v různých stavech.

Stavový diagram pro exekuci



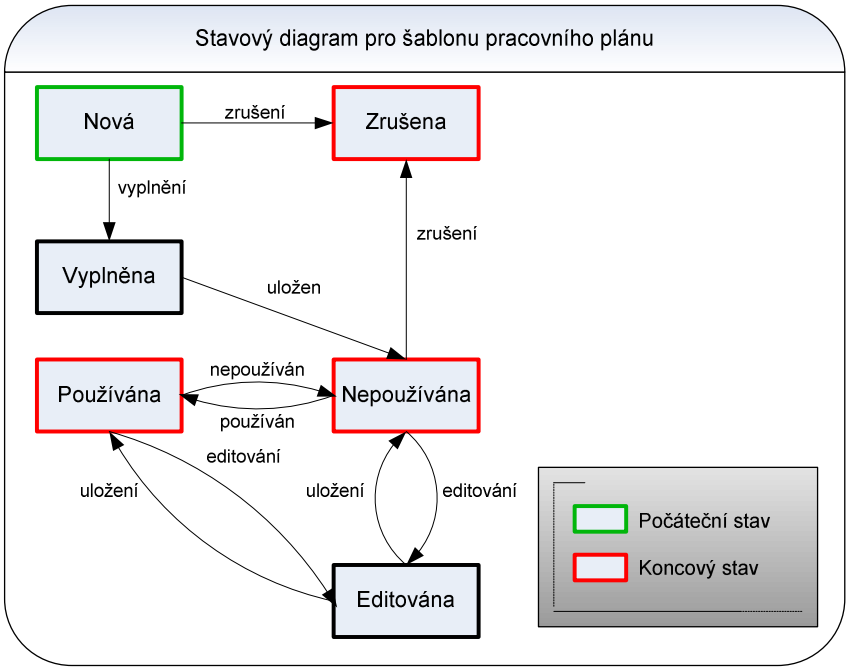
Obrázek 16: Stavový diagram pro exekucí

Stavový diagram přihlášení



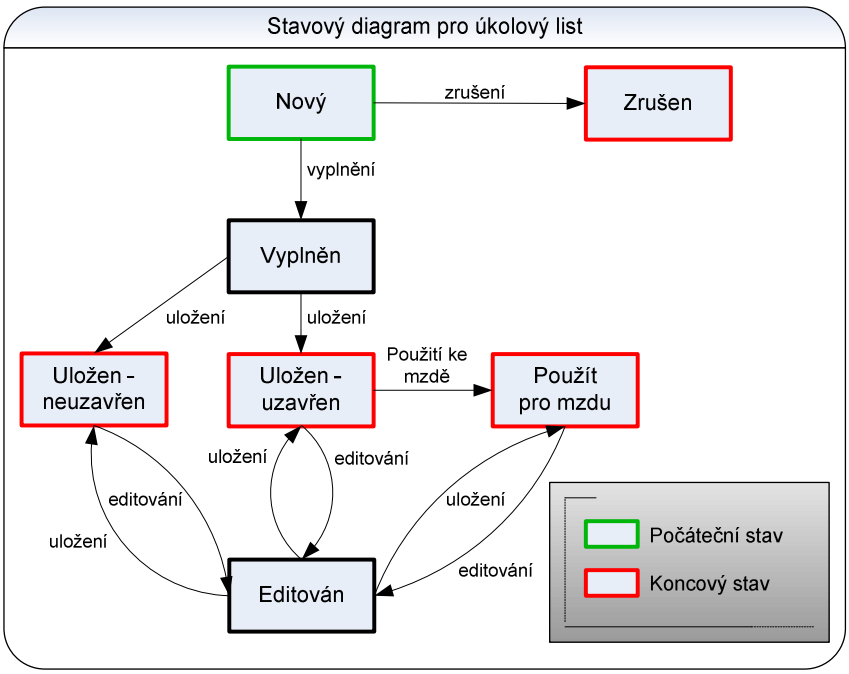
Obrázek 17: Stavový diagram pro přihlášení

Stavový diagram pro šablonu pracovního plánu



Obrázek 18: Stavový diagram pro šablonu pracovního plánu

Stavový diagram pro úkolový list



Obrázek 19: Stavový diagram pro úkolový list

6 Návrh implementace

Dalším krokem po datové analýze se tato práce zabývá návrhem implementace. Zde je nutné řešit technické a programové prostředky kladené na informační systém. Taky už bylo nutné si promyslet grafické rozhraní informačního systému. Dále by se tato práce měla zabývat problémem bezpečnostních otázek. Tato fáze vývoje je důležitá především proto, že by měla později zefektivnit implementaci systému.

6.1 Technické vybavení

Pro efektivní běh aplikace je nutné zvolit vhodné technické vybavení. Hlavní činitel pro výběr vhodného hardwaru je výkon, který je závislý na náročnosti aplikace a především na počtu připojených uživatelů. Největším problémem pro stanovení vhodného vybavení je cena. Velmi výkonné vybavení může jít až do několika set tisíc korun. Proto bych navrhoval pro dané nasazení informačního systému udělat analýzu předpokládaného počtu uživatelů. Na základě analýzy bych navrhnul technické vybavení, které bych posléze otestoval výkonnostními testy pro danou zátěž. Touto cestou bych se snažil optimalizovat výkon za nejnižší cenu.

Pro demoverzi implementovaného systému postačuje webhosting[128]. Pro doimplementování, ladění, testování a prezentaci informačního systému je to dostačující řešení. Na ostré nasazení je i spolehlivý webhosting značně nevhodný z pohledu bezpečnostních otázek. Tento systém bude uchovávat osobní citlivá data, proto je velmi důležitá ochrana těchto dat. Webhosting nám tuto ochranu nezabezpečí. Navrhoval bych pro ostrý provoz sestavit bezpečnostní politiku pro tento systém.

6.2 Softwarové vybavení

Pro výběr softwarového vybavení je největším faktorem cena, pak rychlost a bezpečnost. Většina firem je zařízena na určité softwarové vybavení, u kterého chtějí nadále zůstat. Dalším důležitým faktorem je programovácí jazyk, ve kterém má být systém implementován. Každý programovací jazyk má určité přednosti a nedostatky pro daný druh projektu. Proto je nutné taky přemýšlet o vhodnosti daného programovacího jazyku. Pro implementaci informačního systému zadaného diplomovou práci jsem zvolil technologii .NET. programovací jazyk jsem zvolil C#. Tuto technologii jsem se rozhodl naučit z důvodu oblíbenosti u velkých informačních

[128] webhosting – je pronájem prostoru pro webové stránky na cizím webovém serveru

systému. Alternativou pro technologii .NET by mohla být technologie JAVA[129]. Skriptovací jazyky pro takhle rozsáhlou aplikaci jsem zavrhnul.

V technologii .NET je dobře propracován model logické vrstvy. Logická vrstva aplikace je množina spolupracujících služeb rozdělena do těchto skupin:

- Uživatelské služby (User Services) – tato vrstva slouží jako článek mezi uživatelem a aplikační službou. Tato vrstva tedy zprostředkovává interakci mezi klientem nebo jiným systémem a informačním systémem – programem.
- Aplikační služby (Business Services) – tato vrstva se stará o hlavní funkce systému – programu. Jedná se o zapouzdření aplikační logiky do tzv. komponent.
- Datové služby – tato vrstva poskytuje přístup k datům pomocí obecně použitelných rozhraní.

Proto by mělo být maximální využití těchto vlastností. Vzhled aplikace by tedy měl být definován pomocí aspx stránek, využití témat v .NET technologii a použití CSS stylů.

Pro úložiště dat máme na výběr z velkého množství databázových serverů. Jelikož se jedná o rozsáhlou aplikaci, zavrhnul jsem menší databázové servery jako MySQL[130], SQLLite[131], PostgreSQL[132] a podobně. Mezi větší databázové servery, které nám nabízejí větší možnosti pro tvorbu obrovských databázových systému, můžu uvést firmy jako Oracle[133], IBM[134], Microsoft[135]. Pro implementaci informačního systému jsem se rozhodl použít Microsoft SQL[136] server. Rozhodnul jsem se pro použití Microsoft SQL server z důvodu největší podpory ze strany technologie .NET. Udává se, že použití konektoru pro Microsoft SQL server má být až o 10% rychlejší než použití konektoru třetích stran. Dalším důvodem je využití školní licence, kterou jako student disponuji.

Pro výstupní sestavy z informačního systému byl zvolen formát pdf. Tento formát má mnoho výhod, pro které byl zvolen. Jedná se o platformovou nezávislost, není závislý na typu internetového prohlížeče, dobrá správa a uchovávání dokumentů v elektronické podobě a většina programu pro prohlížení a tisk těchto dokumentů je zdarma.

[129] JAVA – platforma zastřešující různé varianty použití programovacího jazyka JAVA
[130] MySQL – SQL server
[131] SQLLite – SQL server
[132] PostgreSQL – SQL server
[133] Oracle – firma s oblasti informačních technologií – hlavní zaměření na databáze
[134] IBM - firma s oblasti informačních technologií
[135] Microsoft - firma s oblasti informačních technologií
[136] SQL – strukturovaný dotazovací jazyk (Structured Query Language)

6.3 Problematika víceuživatelského přístupu

U systému takového rozsahu a návrhu by měla být řešena problematika víceuživatelského přístupu, pokud bude k systému přistupovat více uživatelů. Vzhledem k tomu, že navrhovaný systém by měl sloužit pro malé až střední firmy, nepředpokládá se, že by ke stejným datům přistupovalo více uživatelů (Každý uživatel bude mít svoje evidované firmy, ke kterým bude mít přístup. Nepředpokládá se, že by malá firma měla vice mzdových účetních.). Tato problematika by i přesto do budoucnosti měla být řešena, pokud by došlo k rozšíření možnosti systému. Problém s víceuživatelským přístupem může být pouze u přístupu uživatele s roli „Mistr“ a zároveň uživatele s roli „Mzdový účetní“ nad stejným úkolovým listem. Tedy pokud by oba uživatele v stejnou chvíli chtěli zadávat hodnoty, mohlo by dojít ke zkreslení výsledku. K téhle situaci by po zavedení víceuživatelského přístupu nemělo dojít.

U databázového serveru Microsoft SQL server je provádění transakcí automaticky zapnuté a tento relační databázový stroj transakce plně podporuje. Veškerá změna v datech vždy probíhá v transakci. Pokud se jedná i o jeden příkaz, tak je z bezpečnostního důvodu úspěšného provedení příkazu uzavřen do transakce. Tedy není-li příkaz uzavřen do explicitní transakce, bude příkaz proveden v takzvaném „Autocommit“ módu.

Microsoft SQL server rozlišuje dva druhý transakcí:

- *Explicitní transakce* – Používá se, pokud je zapotřebí provést více operací v datech jako jeden celek. Začátek a konec transakce je ohraničen příkazem BEGIN TRAN a COMMIT (případně ROLLBACK). Kód kódu může vypadat například:

```
BEGIN TRAN
      BEGIN TRY
            //změna v datech - vykonaný kód
            COMMIT
      END TRY
      BEGIN CATCH
            //Nastala chyba - potřeba se vrátit - ROLLBACK
            ROLLBACK
      END CATCH
END TRAN
```

Obrázek 20: Explicitní transakce

Tyto explicitní transakce mohou být vnořené. Tedy v těle jedné transakce může být další transakce. Toho lze zájmena využít při psaní uložených procedur, které využívají vlastní transakce. Tyto procedury mohou být následně volané bez ohledu na to, zda volající proces má nebo nemá otevřenou transakci.

- *Implicitní transakce* – MS SQL server[137] dokáže implicitně otvírat transakce jako např. Oracle. Tento mód se musí povolit v nastavení příkazem „SET IMPLICIT_TRANSACTIONS ON;”. Implicitní transakce pracují následovně: každý příkaz v rámci připojení otevře novou transakci, pokud žádná není v daném okamžiku otevřena. Pokud už nějaká transakce otevřená je, daný příkaz se provede v dané transakci a neotvírá už novou. Uzavření transakce musí být vždy explicitně pomocí příkazu COMMIT (případně ROLLBACK).

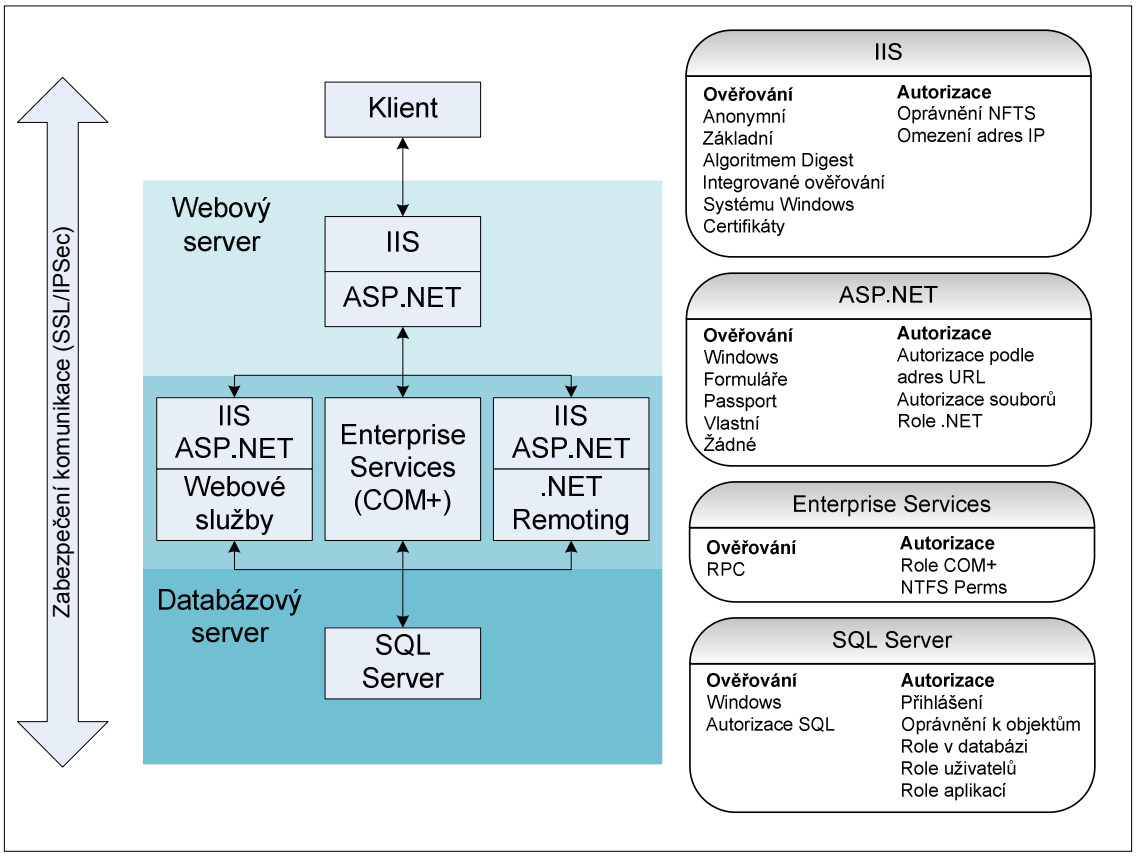
6.4 Návrh bezpečnostních opatření

Otázka bezpečnostního opatření je velmi rozsáhlá. Základy bezpečnosti jsou popsané v úvodu této práce, kde bezpečnost je naznačena jen z malé části oblasti autentizace a autorizace. Nastudovat a popsat bezpečnostní otázky by bylo velmi rozsáhlé a zabralo by nejednu vlastní práci.

Bezpečnostní otázkou je dobré se zabývat i z malé části. Nejlepší řešení je udělat celou bezpečnostní politiku dané firmy. Je třeba chránit data před zneužitím či odcizením. Dále se musí taky udělat zabezpečení dat proti odcizení, živelným pohromám a podobně. U mnoha projektů si nemůžeme dovolit provozní výpadek serveru, proto tedy musíme řešit problémy po stránce spolehlivosti. U IS pro mzdovou a personální agendu by sebemenší výpadek znamenal velké nepříjemnosti a řadu problému. Nemělo by se taky zapomínat na zálohu dat. Ta je důležitá, aby nedošlo k znehodnocení dat v důsledku poruchy.

Při vývoji webové aplikace v prostředí .NET je možné použít různé technologie případně produkty. Tyto technologie na jednotlivých vrstvách aplikace nabízejí základní možnosti ověření a autorizace. Na následujícím obrázku jdou vidět různé přístupy k ověřování a autorizaci na různých vrstvách webové aplikace.

[137] MS SQL Server – Microsoft SQL Server



Obrázek 21: Technologie .NET

Zabezpečení přístupu k datům

Největší problémy při přístupu k datum lze rozdělit do těchto skupin:

- zabezpečené úložiště pro spojovací řetězce – spojovací řetězce obsahující uživatelské jméno a heslo jako prostý text
- Užití vhodné identity pro přístup k databázi
- Přenos dat mezi aplikačním serverem a databázovým serverem – vhodné použít SSL, IPSec nebo serverové certifikáty
- Ověřování a autorizování volajících v databázi
- SQL injection – ochrana proti útokům pomocí vložení škodlivého kódu do SQL příkazu

V tomto informačním systému jsem se snažil SQL injection eliminovat. Základní myšlenkou je, že by se neměly přímo vkládat údaje do SQL dotazu ze vstupu. Nebezpečné vložení cizího kódu může mít za následek zobrazení citlivých dat nebo zničení obsahu databáze.

Nevhodné:

```
string queryString = "UPDATE Address SET city = address.city,...";

string queryString = "UPDATE Address SET city = TextBox_city.Text,...";
```

Vhodné:

```
string queryString = "UPDATE Address SET city = @city, zipcode = @zipcode,...";
SqlCommand dbCommand = new SqlCommand();

dbCommand.Connection = dbConnection;
dbCommand.CommandText = queryString;

dbCommand.Parameters.Add("@city", SqlDbType.VarChar);
dbCommand.Parameters["@city"].Value = address.City;

dbCommand.Parameters.Add("@zipcode", SqlDbType.Int);
dbCommand.Parameters["@zipcode"].Value = address.Zipcode;
```

Obrázek 22: Eliminace SQL injection

Vhodné je testovat vstupní data z formulářů dříve než je použijeme. Data by měla být validována na: datový typ, povolenou znakovou sadu, minimální a maximální délku, kontrola nuly zda je dovolena, nutnost vyplnění vstupu, zda jsou duplikáty povoleny, numerický rozsah a specifické vzory. Většinou se používá JavaScript[138] na straně klienta. V prostředí .NET máme k dispozici validační prvky.NET, které provádějí validaci na straně klienta i serveru (nutné kontrolovat zda je stránka validní – *Page.IsValid*). Dobré je taky kontrolovat vstupy regulárním výrazem nebo můžeme provést přetypování na potřebný datový typ.

Dalším problémem může být přetečení zásobníku. Tedy útočník se pokouší provést přetečení zásobníku, aby mohl spouštět kód v datech, která by měla být zpracována, nikoliv vykonána. Do těchto dat útočník vloží předpřipravený kód a spustí tak útok vůči systému. Pro ochranu je potřeba používat bezpečné knihovny a řádně testovat systém. Řádné testování by mělo kontrolovat délku vkládaných dat a to z důvodu, aby nedocházelo k přetečení zásobníku.

Základní problém nastává taky při nesprávném ošetření chyb v systému. Například mohou být chyby z přístupu k databázi zaslány útočníkovi. Nebo dochází při chybách k odhalení implementačních detailů. Například chyba pro nalezení souboru nám může poskytnout informace o cestě. Ochrana je zobrazování chyb jen pro vývojáře a testery a uživatelům přesměrovávání chyb na hlavní chybovou stránku.

[138] JavaScript – objektově orientovaný skriptovací jazyk

Zabezpečení komunikace

Pro zabezpečení komunikace by bylo vhodné nastavit protokol SSL na webovém serveru. Pro testování IS pro personální a mzdovou agendu na bezplatném webhostingu toto nastavení není možné. Nastavení na serveru by bylo nezbytné pro využití tohoto systému. Protokol SSL je postaven na základu kryptografických technologii. Zajišťuje nám ověřování, utajení a integritu dat. Nejdříve je nutné vytvořit pravdivý certifikát například ve Windows přes IIS[139] – internetovou informační službu. Následně je potřeba nechat tento certifikát podepsat vhodnou certifikační autoritou. Dále pak se tento certifikát nainstaluje do IIS a ještě je potřeba nastavit virtuální adresář webové služby na zabezpečený protokol SSL.

Pokud by bylo potřeba ověřovat uživatele nebo jiné přistupující aplikace na vyšší úrovni než pomocí hesel, je vhodné použít klientské certifikáty. K tomuto je potřeba mít nainstalován serverový certifikát. Dále je potřeba v ve Windows v IIS nastavit v dialogu *zabezpečená komunikace* políčko *vyžadovat zabezpečený kanál (SSL)*. Dále je potřeba ještě nastavit *vyžadovat klientské certifikáty*. Klientský certifikát může být podepsán jakoukoliv certifikační autoritou. Pokud klientský certifikát nemáme, je potřeba o tento certifikát požádat a nainstalovat na klientský počítač.

V prostředí .NET lze certifikát ověřit například:

```
string ret = String.Empty;
HttpClientCertificate cert = this.Context.Reguest.ClientCertificate;

If(cert.IsPresent)
{
      ret = "Subject: " + cert.Subject;
      ret = ret + ", SubjectCN: " + cert.Get("SUBJECTCN");
      ret = ret + ", SubjectOU: " + cert.Get("SUBJECTOU");
      ...
      return ret;
}
```

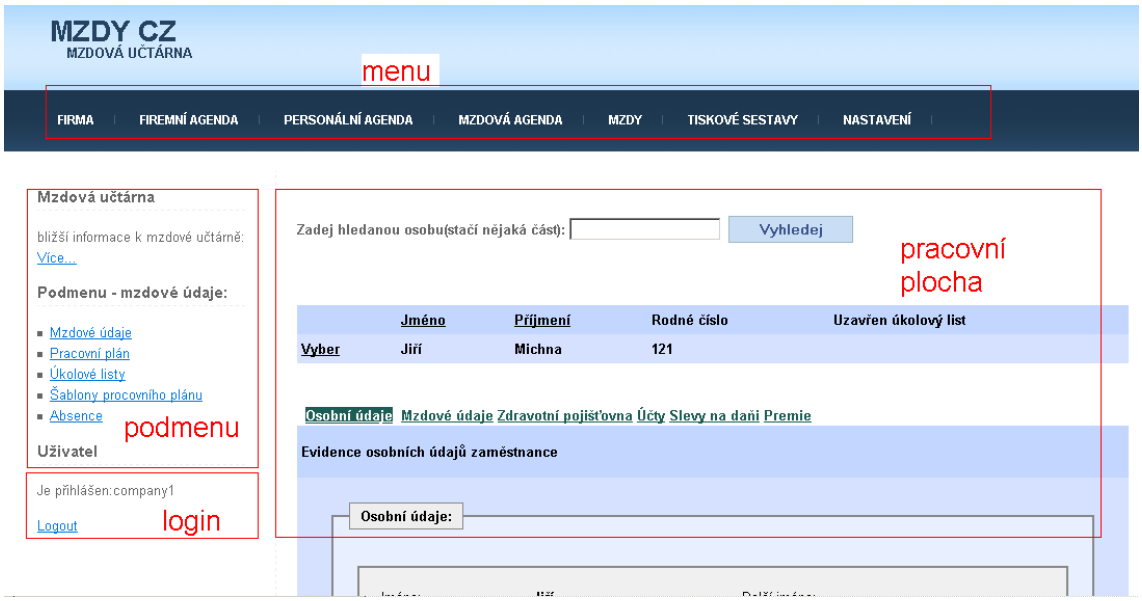
Obrázek 23: .NET ověření certifikátu

6.5 Grafický návrh

Návrh implementace zahrnuje taky návrh grafického prostředí. Pro tento návrh bylo zvoleno rozvržení zón do několika oblastí. Grafické rozvržení by mělo být pro celou aplikaci pokud možno jednotné. Uživatelská tlačítka by měla být také ve stejném pořadí. Tato pravidla by měla zlepšit a urychlit orientaci v uživatelském prostředí.

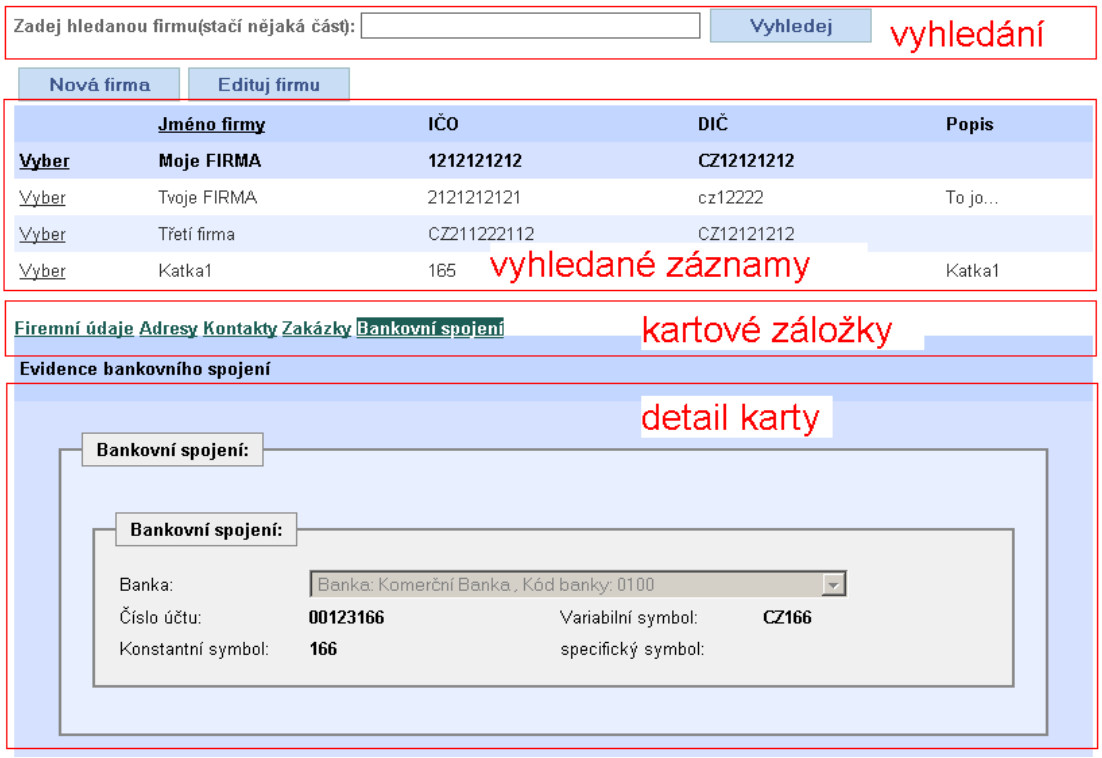
[139] IIS – informační server pro internet (Internet Information Server)

Vzhled aplikace je rozdělen do 4základních částí. Jedná se o hlavní menu s hlavními položkami pro navigaci. Každá položka hlavního menu následně obsahuje podmenu v levé části aplikace. Zde jsou další podpoložky aplikace pro dané menu. V části podmenu je rychlá orientace přihlášeného uživatele a možnost ohlášení. Ještě je zde pracovní plocha kde se nachází prostor pro aktivní obsah.



Obrázek 24: Grafický návrh 1

Pracovní plocha je většinou rozdělena na další zóny. Jednak tu je zóna pro vyhledání objektů. Další zóna obsahuje seznam vyhledaných objektů. Pro vybraný objekt je možnost přepínat v menu obsahující kartové záložky. Tyto kartové záložky jsou inspiraci ze stolních aplikací a měly by v uživateli navodit dojem práce se stolní aplikací. Následně pod kartovými záložkami se nachází prostor pro detail karty.



Obrázek 25: Grafický návrh 2

Aplikace by měla podporovat témata vzhledů pro aplikaci barevného schématu pro danou osobu. Každé osobě vyhovuje jiné barevné ladění, a proto tato vlastnost by měla zpříjemnit práci s aplikací.

6.6 Návrh komponenty úkolového listu

Pro vývoj tohoto informačního systému jsem zvolil vývoj samostatné komponenty pro úkolový list. Bylo to z důvodu generování měsíčního kalendáře, kde každý den bude obsahovat stejnou množinu atributů a funkcí. Komponenta představuje jeden den pro zadávání hodinových hodnot pro mzdovou agendu. Komponenta je vytvořena zvlášť a následně využita v informačním systému pro úkolový list. Komponenta musí být schopna načítat zakázky a jejich barvy pro evidované firmy. Dále musí být schopna měnit svůj stav pro zadávání odpracované doby pro jednotlivé zakázky, dále nemocenskou ve třech režimech, dovolenou, neomluvenou absenci, omluvenou absenci a překážku v práci. Hodnoty by měly být reálná čísla s přesností na jedno desetinné číslo.

6.7 Tiskové sestavy

Pro informační systém byla navržená základní sada tiskových sestav jako je jednoduchý a podrobný seznam zaměstnanců, detail zaměstnance, detail dítěte osoby, jednoduchý a podrobný seznam firem, detail firmy, seznam zakázek firmy, výplatní list, rekapitulace mezd – sociální pojištění, přehled o výši pojistného a vyplacených dávkách, rekapitulace mezd – výplaty, přehled pro zdravotní pojišťovny, mzdový list, potvrzení o zdanitelných příjmech ze závislé činnosti z a funkčních požitků srážených záloh na daň a daňovém zvýhodnění. Tyto sestavy by měla pokrýt potřebné dokumenty pro zaměstnance, Finanční úřad, pro Českou správu sociálního zabezpečení a pro Zdravotní pojišťovny.

Sestavy jsou navržené pro výstup ve formátu pdf[140]. Také je možnost exportovat sestavy do formátu xls[141].

[140] pdf – přenosový formát dokumentů vyvinutý firmou Adobe(Portable Document Format)

[141] xls – je přípona souborů specifikace Office Open XML vytvořená v aplikaci Microsoft Excel

7 Implementace

Implementace probíhala v několika iteracích. Nejdříve bylo nutné vytvořit formuláře pro sběr dat do systému. Jako první jsem vytvořil formuláře pro firemní agendu. Následně jsem začal vytvářet personalizaci, členství a správu rolí, zabezpečení, autentizaci a autorizaci. V další iteraci byla vytvořena personální agenda a dále jsem začal tvořit komponentu pro úkolový list. Když byla komponenta dokončena, zahájil jsem vytvářet mzdovou agendu pro sběr dat ohledně mezd. Základní formuláře pro prohlížení, sběr a editaci dat byly vytvořeny, a tak jsem pokračoval implementovat úkolový list a testovat komponentu. Následně jsem vytvořil oddíl pro výpočet mezd a načítání hodnot z úkolového listu. V závěru bylo nutné doimplementovat tiskové sestavy a administrátorské rozhraní pro správu číselníku, účtů a rolí.

Další informace o implementaci demonstračního informačního systému je možné čerpat z programátorské příručky umístěné na přiloženém CD. V programátorské příručce jsou popsané jednotlivé funkce a soubory. Dále je sepsaná uživatelská příručka k informačnímu systému, která je přiložena na CD a také v programu jako nápověda. Na přiložené CD jsem taky umístil veškeré kódy vytvořené aplikace, kódy vytvořené komponenty, potřebné knihovny a programy. Na CD je také přiložena databáze v datovém souboru *DatabasePayroll.mdf*.

K implementaci jsem využil několik informačních zdrojů. Jedna se o knihy CSS a XHTML : tvorba dokonalých webových stránek krok za krokem [3], ASP.NET a ADO.NET 2.0. : hotová řešení [5], Vytváříme zabezpečené aplikace v Microsoft ASP.NET [6], ASP.NET 2.0 : programujeme profesionálně [7] a C# 2005 : programujeme profesionálně [8]. Dále jsem čerpal z internetových zdrojů [55], [56], [57], [58] a [59].

7.1 Použité programové vybavení

Vývoj aplikace:

operační systém	Microsoft Windows XP SP[142]2
www server	integrovaný web server Microsoft Visual Studio 2005 v. 8.0.50727.42
programovací jazyk	C#
.NET framework	2.0.50727
databáze	Microsoft SQL Express server 2005
vývojové prostředí	Microsoft Visual Studio 2005 v. 8.0.50727.42

[142] SP – Service Pack

grafický editor	Paint.NET v3.36 GIMP 2.4.5
internetový prohlížeč	Mozilla Firefox verze 3.0.7

Pro sestavení dokumentace:

textový editor	Microsoft Word 2007
tabulkový editor	Microsoft Excel 2007
tvorba diagramů, obrázků	Microsoft Visio 2007

Pro běh demoverze na internetu:

operační systém	Windows 2003 Server
www server	Internet Information Server 6.0
databázový server	Microsoft SQL Express server 2005
.NET framework	2.0

7.2 Umístění demoverze

Demoverzi informačního systému jsem pro ukázku umístil na freehostingovou službu na adrese http://mzdy.aspweb.cz/. Data umístěna v informačním systému jsou smyšlená. Do aplikace je možné přidávat vlastní testovací data. Aplikace je testována v prostředí Mozilla Firefox verze 3.0.7, který je doporučován a Opera verze 9.64. Další testovací prohlížeč byl Internet Explorer 6.0. Tento prohlížeč lze používat, ale má drobné odlišnosti v interpretaci CSS stylů.

7.3 Obsah přiloženého CD

/root/

- abstraktCZ.txt	- Abstrakt v českém jazyce
- abstractEN.txt	- Abstrakt v anglickém jazyce
- klicova_slovaCZ.txt	- Klíčová slova v českém jazyce
- key_wordsEN.txt	- Klíčová slova v anglickém jazyce
- obsah_CD.txt	- Obsah CD
/docs/	- Adresář pro dokumenty

/ms_word/	- Dokumentace formátu MS WORD
- diplomova_prace.doc	- Elektronická verze diplomové práce
- dokumentace_prog.doc	- Programátorská dokumentace
- dokumentace_uziv.doc	- Uživatelská dokumentace
/pdf/	- Dokumentace formátu pdf
- diplomova_prace.pdf	- Elektronická verze diplomové práce
- dokumentace_prog.pdf	- Programátorská dokumentace
- dokumentace_uziv.pdf	- Uživatelská dokumentace
/documentation/	- Dokumentace k implementaci
/attachments/	- Adresář pro přílohy k diplomové práci
/precompiled_web/	- Adresář předkompilované aplikace IS
/web_sites/	- skripty aplikace IS

8 Závěr

Na začátku této práce jsem o problematice mzdového účetnictví nevěděl nic, proto diplomová práce byla pro mě něco nového a zajímavého. Mnoho zaměstnanců i zaměstnavatelů našeho státu neznají postup pro výpočet mezd. V době informačních technologií a systému pro mzdovou a personální agendu tento přehled ztrácejí i odborníci na tuto problematiku a v případě nejasností hledají informace v zákoníku práce a dalších zákonech. Proto jsem musel na začátku přečíst zákoník práce a naučit se orientovat v něm. Na začátku bylo také potřeba projít a vyzkoušet si několik programů zabývajících se personální a mzdovou agendou. Také bylo potřeba na začátku prostudovat zákon o ochraně osobních dat, neboť zaměstnavatelé přecházejí do styku s velkým množstvím personálních dat.

Velkou část času jsem věnoval problematice datové analýzy systému. Bylo nutné navrhnout databázové schéma pro evidování údajů personální a mzdové agendu. Toto základní jádro databáze obsahuje okolo 60 tabulek a následně by mohlo docházet k rozšiřování o evidenci dalších údajů. Pro základní analýzu jádra systému byla provedena také funkční a časová analýza.

Část této diplomové práce jsem věnoval problematice bezpečnosti informačních systémů. Vzhledem k tomu, že aplikace je navrhnuta pro běh v internetovém prostředí, je potřeba zajistit důvěryhodnost komunikujících osob. Nesmí dojít k odcizení citlivých dat a také je potřeba zajistit spolehlivost provozu systému. Implementování systému běží na bezplatné webhostingové službě, a proto je nutné řešit problém implementace bezpečnostních prvků. Touto částí se zabývám převážně teoreticky.

Implementace jádra systému proběhla v prostředí Microsoft .NET a není komplexním systémem. Při realizaci informačního systému jsem se zaměřil pouze na realizaci tarifních (měsíční, hodinová) mezd. Na doporučení mzdové účetní jsem se pro složitost a různorodost do úkolových mezd nepouštěl, tyto umí převážně jen velké systémy. Problémem exekucí a nařízených srážek ze mzdy jsem se zabýval také pouze okrajově. Tato problematika je složitá a programově obtížně implementovatelná. V implementovaném systému dochází k strhávání exekucí a srážek ze mzdy, ale rozhodnutí oprávněnosti strhnutí už je na obsluze.

V dalším vývoji a implementaci systému, bych nutně navrhoval blízkou spolupráci se mzdovou účetní pro rozvoj a uspořádání dalších funkcí. Pokud by mělo dojít k nasazení systému (i momentálně doimplementované verze systému) do ostrého provozu, je nutná konzultace s odborníkem přes mzdovou a personální problematiku v oblasti správného vysvětlení a implementace mzdových zákonů. Také bych dále navrhoval provést funkční a výkonové testy aplikace.

Bc. Antonín Hlosta

Seznam obrázků

Seznam tabulek

Literatura a informační zdroje

Bibliografie

[1] Šarmanová, J.: *Teorie zpracování dat*. Skriptum VŠB-TUU, Ostrava 1997

[2] PECINOVSKÝ, Jan, PECINOVSKÝ, Rudolf. *Word7 pro Windows 95 : snadno a dobře*. 1. Dotisk vyd. Praha 1 : Grada Publishing, spol. s.r.o., 1997. 256 s. ISBN 80-7169-325-1.

[3] DRUSKA, Peter. *CSS a XHTML : tvorba dokonalých webových stránek krok za krokem*. 1. vyd. Praha : Grada Publishing, a.s., 2006. 200 s. Průvodce. ISBN 80-247-1382-9.

[4] BOŘIVOJ, Šubrt, et al. *ABECEDA mzdové účetní : edice práce, mzdy, pojištění*. 18. vyd. [s.l.] : ANAG, 2008. 534 s. ISBN 978-80-7263-438-5.

[5] LACKO, Luboslav. *ASP.NET a ADO.NET 2.0. : hotová řešení*. Brno : Computer Press, a.s., 2006. 381 s. ISBN 80-251-1028-1.

[6] *Vytváříme zabezpečené aplikace v Microsoft ASP.NET*. Bogdan Kiszka. Brno : Computer Press, 2004. 542 s. ISBN 80-251-0466-4.

[7] BILL, Evjen, et al. *ASP.NET 2.0 : programujeme profesionálně*. Karel Voráček. Brno : Computer Press, a.s., 2006. 1224 s. ISBN 978-80-251-1473-5.

[8] NAGEL, Christian, et al. *C# 2005 : programujeme profesionálně*. Jakub Mikulaštík, Petr Dokoupil. Brno : Computer Press, a.s., 2006. 1398 s. ISBN 80-251-1181-4.

Internetové zdroje

[9] HANÁČEK, Petr, STAUDEK, Jan. http://aplikace.mvcr.cz [online]. 2000 [cit. 2008-12-12]. PDF dokument. Text v češtině. Dostupný z WWW: http://aplikace.mvcr.cz/archiv2008/micr/files/479/uvis_bezpecnost_20000701.pdf

[10] *Ministerstvo vnitra České republiky* [online]. c2005 [cit. 2009-04-15]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://web.mvcr.cz/archiv2008/sbirka/>.

[11] *Podnikatel.cz : business Server* [online]. c2007-2009 [cit. 2009-02-02]. Kódováno v iso-8859-2. Text v češtině. Dostupný z WWW: < http://www.podnikatel.cz/zakony/zakon-c-262-2006-sb-zakonik-prace/>. ISSN 1802-8012.

[12] *Bussines.center.cz* [online]. HAVIT s.r.o., c1998-2009 [cit. 2009-04-15]. Kódováno ve UTF-8. Text v češtině. Dostupný z WWW: <http://business.center.cz/business/pravo/zakony/>. ISSN 1213-7235.

[13] *Ministerstvo práce a sociálních vecí* [online]. [2005] [cit. 2009-02-10]. Kódováno ve UTF-8. Text v češtině. Dostupný z WWW: <http://www.mpsv.cz/cs/>.

[14] FRANTIŠEK, Jirásek. *Bílý Újezd : Dějiny obce s připojenou osadou Roudné* [online]. c2007 [cit. 2008-12-12]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://www.bilyujezd.cz/bu/kronika/>.

[15] *Rovné šance* [online]. [cit. 2009-04-15]. Kódováno ve UTF-8. Text v češtině. Dostupný z WWW: <http://www.rovnesance.cz/rovne-sance>.

[16] *Měšec.cz : Server o osobních financích* [online]. c1999-2009 [cit. 2009-02-01]. Kódováno v iso-8859-2. Text v češtině. Dostupný z WWW: <http://dane.mesec.cz/>. ISSN 1213-4414.

[17] *BusinessInfo.cz : Oficiální portál pro podnikání a export* [online]. CzechTrade, c1997-2009 [cit. 2009-02-04]. Kódováno ve UTF-8. Text v češtině. Dostupný z WWW: < http://www.businessinfo.cz/cz/rubrika/finance-dane/1000433/>.

[18] *Finance.cz : Poznejte hodnotu informace* [online]. AWD Česká republika, c2000-2009 [cit. 2009-02-02]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://www.finance.cz/>. ISSN 1213-4325.

[19] *Výplata : mezd, sociálních podpor a důchodů...* [online]. SVT Brno, s.r.o., c2002-2009 [cit. 2009-02-02]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://www.vyplata.cz/>.

[20] VÁCLAV, Němec. *Dějepis.com* [online]. c2007-2009 [cit. 2009-02-02]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://www.dejepis.com/index.php>.

[21] *Svět sítí : O počítačových sítích nejen pro administrátory a specialisty* [online]. c2000-2009 [cit. 2008-12-10]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://www.svetsiti.cz/view_list.asp?rubrika=Tutorialy&temaID=264>.

[22] *Interval.cz : webdesing a e-komerce denně* [online]. 2002 [cit. 2008-11-20]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://www.axima-brno.cz/index.html>. ISSN 1212-865.

[23] *SMSAgent : SMS komunikace a mobilní marketing* [online]. AXIMA, spol. s.r.o., [2008] [cit. 2008-12-15]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://www.smsagent.cz/>.

[24] *Visualtron : VisualGSM* [online]. c2002-2008 [cit. 2008-12-12]. Text v angličtině. Dostupný z WWW: <http://www.visualgsm.com/index.htm>.

[25] KRHOVJÁK, Jan, et al. *Zpravodaj ÚVT MU* [online]. 2007 [cit. 2008-12-18]. Kódováno v iso-8859-2. Text v češtině. Dostupný z WWW: <http://www.ics.muni.cz/bulletin/articles/562.html>.

[26] *I.CA a.s.* [online]. I.CA a.s., c2000-2008 [cit. 2008-11-16]. Kódováno ve UTF-8. Text v češtině. Dostupný z WWW: <http://www.ica.cz/home_cs/?acc=teorie_a_principy>.

[27] STEINBERGER, Josef. *Zapracování digitalního podpisu pro autentizaci přístupu Oracle Portal*. Plzeň, 2003. 149 s. Diplomová práce. Dostupný z WWW: <http://www.kiv.zcu.cz/~jstein/projekty/diplomka.pdf>.

[28] *PC svět* [online]. [2008] [cit. 2008-11-10]. Text v češtině. Dostupný z WWW: <http://www.pcsvet.cz/art/article.php?id=3355>.

[29] *I.CA a.s.* [online]. I.CA a.s., c2000-2008 [cit. 2008-11-16]. Text v češtině. Dostupný z WWW: <http://www.ica.cz/home_cs/?acc=casova_razitka>.

[30] *I.CA a.s.* [online]. I.CA a.s., c2000-2008 [cit. 2008-11-16]. Text v češtině. Dostupný z WWW: <http://www.ica.cz/home_cs/?acc=casova_razitka_a_casove_autority>.

[31] *Instalace certifikační autority* [online]. 22.11.2002 [cit. 2008-11-16]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://uvt1.cuni.cz/ca/>.

[32] FIALA, Martin. *Certifikační autorita* [online]. [2003] [cit. 2008-11-16]. Text v češtině. Dostupný z WWW: <http://hosting.ok.cvut.cz/~digri/ca.pdf>.

[33] *Certifikační autorita Czechia* [online]. c2003-2004 , 31.10.2008 [cit. 2008-11-16]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://www.caczechia.cz/default.asp>.

[34] RůŽIČKA, Pavel. *Bezpečnost především - použití SLL* [online]. 6.6.2002 [cit. 2008-11-16]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://interval.cz/clanky/bezpecnost-predevsim-pouziti-ssl/>.

[35] *Zabezpečené připojení pomocí protokolu SSL* [online]. Microsoft Corporation, c2009 [cit. 2008-12-16]. Text v češtině. Dostupný z WWW: <http://technet.microsoft.com/cs-cz/library/cc739306.aspx>.

[35] *Svět sítí : SSL protokol* [online]. Svět sítí & Infinity, a.s., c2000-2009 [cit. 2008-11-16]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://www.svetsiti.cz/view_list.asp?rubrika=Tutorialy&temaID=171>.

[36] *Certifikační autorita a OpenSSL : digiweb* [online]. 24.1.2007 [cit. 2008-11-16]. Kódováno ve UTF-8. Text v češtině. Dostupný z WWW: <http://digiweb.ok.cvut.cz/bezpecnost/certifikacni-autorita-s-openssl>.

[37] KÁRA, Michal. *Jak na OpenSSLII* [online]. 2.5.2003 [cit. 2008-11-16]. Kódováno v iso-8859-2. Text v češtině. Dostupný z WWW: <http://www.root.cz/clanky/jak-na-openssl-2/>. ISSN 1212-8309.

[38] *PC svět* [online]. [2008] [cit. 2008-11-10]. Text v češtině. Dostupný z WWW: <http://www.pcsvet.cz/art/article.php?id=3184>.

[39] *I.CA a.s.* [online]. I.CA a.s., c2000-2008 [cit. 2008-11-16]. Text v češtině. Dostupný z WWW: <http://www.ica.cz/home_cs/?acc=o_cipovych_kartach>.

[40] PETERKA, Jiří. *EArchiv.cz : Bezpečnostní aspekty interbankingu* [online]. [2001] [cit. 2008-11-16]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://www.earchiv.cz/b01/b0600005.php3>.

[41] VRBA, Marek. *Mikroplatby : jaké jsou možnosti?* [online]. 23.5.2007 [cit. 2008-11-18]. Kódováno v iso-8859-2. Text v češtině. Dostupný z WWW: <http://www.lupa.cz/clanky/mikroplatby-jake-jsou-moznosti/>. ISSN 1213-0702.

[42] MACHALA, Karel. *Platby na internetu : změny na obzoru* [online]. 21.9.2006 [cit. 2008-11-18]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://bankovnictvi.ihned.cz/3-19353570-loajalitu-900000_d-32>. ISSN 1213-7693.

[43] *Platba.cz : platební portál* [online]. [2004] [cit. 2008-11-18]. Kódováno ve WIN-1250. Text v češtině. Dostupný z WWW: <http://www.platba.cz/platba.asp?s0=cz&s1=informace&s2=methods&PHPSESSID=df1487a3cc0e8111cfb20f47b2b4728c>.

Přílohy

[44] *ASP.NET security overview* [online]. Microsoft Corporation, 16.11.2007 [cit. 2008-12-05]. Text v angličtině. Dostupný z WWW: <http://support.microsoft.com/kb/891028>.

[45] *Začínáme s ASP.NET 2.0 : 9.díl -autentizace, autorizace* [online]. 22.11.2005 [cit. 2008-12-04]. Text v češtině. Dostupný z WWW: <http://www.zive.cz/ASPASPNET/Zaciname-s-ASPNET-20--9-dil--autentizace-autorizace/sc-70-sr-1-a-127758/default.aspx>. ISSN 1212-8554.

[46] VONDRA, Ondřej. *Porovnání Java a .NET z hlediska bezpečnosti*. [s.l.], 2007. 42 s. Vedoucí bakalářské práce Ing. David Kalita. Dostupný z WWW: <https://dip.felk.cvut.cz/browse/pdfcache/vondro3_2007bach.pdf>.

[47] *Java Security Architecture* [online]. Sun Microsystems, c1997-2002 [cit. 2008-12-12]. Text v angličtině. Dostupný z WWW: <http://java.sun.com/j2se/1.4.2/docs/guide/security/spec/security-specTOC.fm.html>.

[48] MATUŠKA, Miroslav. *Java Authentication and Authorization Service (JAAS)* [online]. [2001-2002] [cit. 2008-12-12]. Text v češtině. Dostupný z WWW: <http://nb.vse.cz/~zelenyj/it380/eseje/xmatm25/JAASfile.htm>.

[49] TICHÝ, Jan. *Aplikační framework phpBASE* [online]. c2004-2009 [cit. 2008-12-13]. Kódováno ve UTF-8. Text v češtině. Dostupný z WWW: <http://www.jantichy.cz/diplomka/phpbase>.

[50] *PEAR - PHP Extension and Application Repository* [online]. c2001-2009 [cit. 2009-01-10]. Text v angličtině. Dostupný z WWW: <http://pear.php.net/>.

[51] *HTTP authentication with PHP* [online]. c2001-2009 [cit. 2009-01-10]. Kódováno ve UTF-8. Text v angličtině. Dostupný z WWW: <http://cz.php.net/features.http-auth>.

[52] KUBIŠ, Michal. *Autorizácia v PHP s MySQL* [online]. 23.10.2003 [cit. 2009-01-10]. Text ve slovenštině. Dostupný z WWW: <http://interval.cz/clanky/autorizacia-v-php-s-mysql/>. ISSN 1212-8651.

[53] TICHÝ, Jan. *Autentizace a autorizace* [online]. c2004-2009 [cit. 2009-01-13]. Kódováno ve UTF-8. Text v češtině. Dostupný z WWW: <http://www.jantichy.cz/vyuka/4iz228/php/autentizace>.

[54] *Oracle database bezpečnostní mechanismy* [online]. [2008] [cit. 2009-01-15]. Text v češtině. Dostupný z WWW: <http://www.oracle.com/global/cz/database/database_security_overview_cz3.pdf>.

[55] *The Code Project* [online]. c1999-2009 [cit. 2009-03-10]. Text v angličtině. Dostupný z WWW: <http://www.codeproject.com/>.

[56] *MSDN* [online]. Microsoft Corporation, c2009 [cit. 2009-03-10]. Text v angličtině. Dostupný z WWW: <http://msdn.microsoft.com>.

[57] *Technická podpora online pro Českou republiku* [online]. Microsoft Corporation, c2009 [cit. 2009-03-10]. Text v češtině. Dostupný z WWW: <http://support.microsoft.com/>.

[58] *ASP.NET QuickStart Tutorial* [online]. c2005-2007 [cit. 2009-03-10]. Text v slovenštině. Dostupný z WWW: <http://quickstart.aspnet.sk/QUICKSTARTV20/aspnet/default.aspx>.

[59] *Regular Expression Library* [online]. c2001-2009 [cit. 2009-03-10]. Text v angličtině. Dostupný z WWW: <http://www.regexlib.com/>.

Přílohy

A. Programy pro zpracování personální a mzdové agendy

Duna/mzdy[143]

Jedná se o program, který zpracovává personální i mzdovou agendu. Program je koncipován a určen pro operační systém Windows. Program je určen pro zpracovávání agend více firem. Systém duna/mzdy je tvořen následujícími agendami:

- Personalistika
- Pracovní poměry
- Děti
- Školení a kurzy
- Stálé srážky
- Stále příspěvky
- Nemocenské dávky
- Měsíční zpracování mezd
- Výstupy
- Archiv
- Výpočty
- Číselníky
- Formuláře
- Statistika – šetření o ceně práce (ŠCP)
- Statistika – informační systém o platech (ISP)
- Servisní akce

[143] http://www.tco.cz/

Mzdy 2008[144]

Tento program je určen pro vedení mzdové agendy pro neomezený počet firem (z logického pohledu). Program nám taky umožňuje provádět personální agendu. Program se dělí na části:

- Personální agenda
- Mzdová agenda
- Tisková agenda
- Firemní nastavení
- Speciální operace

Program je koncipován prostředí Windows.

OK mzdy[145]

OK mzdy je program pro kompletní zpracování mzdové agendy. Tento software obsahuje i personální agendu, ale pouze ve stručné formě. Program je koncipován pro mzdovou agendu více firem. Tento program je navržen v prostředí MS Windows.

Ekonomický software varia[146]

Program určen pro zpracování personální a mzdové evidence v organizacích. Program je v provedení buď do 25 zaměstnanců nebo pro velké firmy. Program je koncipován v prostředí MS Windows.

PC mzdy[147]

Program slouží pro zpracování personální a mzdové evidence a evidence nemocenských dávek. Program je koncipován v prostředí MS Dos.

[144] http://www.ainex.cz/
[145] http://www.oksystem.cz/
[146] http://variasoft.cz/
[147] http://pcmmzdy.cz/

Pamica 2008 - pohoda[148]

Program slouží na vedení agend personalistiky, pracovních poměrů a zpracování mezd zaměstnanců. Lze tento program využít ve spolupráci s účetním programem pohoda nebo i samostatně.

Money S3[149]

Money S3 je komplexní ekonomický systém. Tento program nabízí moduly jako jsou například: podvojné účetnictví i daňová evidence (jednoduché účetnictví), adresář, fakturaci, sklady, objednávky, mzdy a řadu dalších doplňků, včetně homebankingu, propojení s pokladními systémy, internetovými obchody nebo dalšími aplikacemi na bázi XM. Program je koncipován do prostředí MS Windows. Dále program Money S3 nabízí další řadu nástaveb nad tento systém.

Ježek software - účto[150]

Program je koncipován v prostředí MS Dos. Tento program je velmi rozšířen mezi malými podnikateli pro svoji jednoduchost a nízkou cenu. Tento program za zaměřen především na účetnictví, ale obsahuje nabídku pro mzdovou agendu.

Outsourcing mzdového účetnictví

Outsourcing mzdového účetnictví lze rozdělit do dvou skupin. První skupina firem se zabývá poskytováním výpočtů, dodáním podkladů potřebných pro mzdovou agendu. Druhá skupina firem se zabývá kompletní správou mzdové agendy. Tato kompletní správa zahrnuje komunikaci s finančním úřadem, statní správou sociálního zabezpečení, zdravotními pojišťovnami, atd. Dále zahrnuje zastupování při kontrolách souvisejících se mzdou zaměstnanců, evidenční listy důchodového pojištění, vyúčtování záloh na dani, roční zúčtovaní srážkové daně, přihlášení a odhlášení zaměstnanců, statistiky, bezplatné poradenství, atd. Pro tuto komplexní správu je nutné, aby si outsourcingová firma udržovala personální agendu. Touto formou mzdového účetnictví se zabývají např. firmy SEVIN s.r.o.[151] a HAKO – MZDY s.r.o.[152]

[148] http://www.stormware.cz/
[149] http://www.money.cz/
[150] http://www.ucto2000.cz/
[151] www.sevin.cz
[152] www.hako-mzdy.cz

Podpora srovnávaných programů

Název programu	Školení		Poradna (technická podpora)		
	Obsahuje	Cena od	Telefon	E-mail	Jiné
Dana/mzdy	Ano	1500Kč	Ano	Ano	
Mzdy 2008	Ne		Ne	Ano	
OK mzdy	Ano		Ano	Ano	Setkání uživatelů, On-line
Varia					
Pc mzdy					
PAMICA	Ano	1980Kč	Ano	Ano	On-line, fax
Money S3	Ano	1189Kč	Ano	Ano	On-line, servisní smlouva
Účto	Ne		Ano	Ano	

Tabulka: Podpora srovnávaných programů

Systémové požadavky srovnávaných programů

Název programů	Softwarové	Hardwarové			Ostatní
		Procesor	RAM	HDD	
Duna/mzdy	MS Windows: 98, ME, 2000, XP	Pentium IV	512MB	200MB	Min. rozlišení 1024x768
Mzdy 2008	MS Windows 98 a vyšší	Pentium	16MB		
OK mzdy	MS Windows 2000/XP	Pentium 1Ghz	256MB	300MB	Databáze MS Access97
Varia	MS Windows 95 a vyšší	Pentium	32MB	30MB	Min. rozlišení 800x600
PC mzdy	Dos, MS Windows				
PAMICA	MS Windows 98 a vyšší	Pentium 1Ghz	128MB	100MB	Min. rozlišení 800x600
Money S3	MS Windows 200, XP, Vista	Pentium, AMD alespoň 550Mhz	1GB	300MB	Min. rozlišení 1024x768
Účto	Dos, Ms Windows				

Tabulka: Systémové požadavky srovnávaných programů

Licenční podmínky srovnávaných programů

Název programů	Demoverze	Omezení demoverze	Cena plné verze od	Omezení plné verze k počáteční ceně
Duna/mzdy	Ano	Zpracování dat do 2 zaměstnanců	10700Kč	
Mzdy 2008	Ano	60dnů	2400Kč	1licence
OK mzdy	Ano		3950Kč	1licence, do 10zaměstnanců
Varia	Ano	Počet vložených záznamů	2400Kč	Do 20zaměstnanců
PC mzdy	Ano	4měsíce nebo 150zpuštění	1100Kč	Do 5zaměstnanců
PAMICA	Ano		9980Kč	Do 25zaměstnanců
Money S3	Ano	Počet vložených záznamů	4748Kč	Počet vložených záznamů
Účto	Ano	30dní a počet vložených záznamů	3998Kč	
Outsourcing mezd	Ne		cca 170Kč – 380Kč/os./měsíc	

Tabulka: Licenční podmínky srovnávaných programů

Hodnocení programů z osobního hlediska

Duna/mzdy

Personální agenda

Dostatečná množství evidovaných údajů. Horší evidence manželky/manžela - pouze jméno a rodné číslo. Zpracována personální evidence dětí. I při personální agendě dětí nutnost vložit počet dětí pro slevu na dani. Možnost evidence cizinců a také možnost v personální agendě dopsat další text pro každou osobu. Možnost vložení fotky. Kvalitní vyhledávání a sestavy podle různých atributů. Dále agenda školení a kurzů, příspěvky a dary, exekuce, stalé srážky a nemocenské dávky.

Mzdová agenda

Dobře definované mzdové údaje. Evidence dovolené, mateřské, apod. Chybí možnost evidence mzdových listů. Možnost exportů hlášení pro jednotlivé pojišťovny a přihlášky/odhlášky pro ČSSZ. Program nabízí výpočet hrubé a čisté mzdy.

Hodnocení

Program bych po vizuální stránce hodnotil kladně. Po určité době si lze rychle zvyknout na strukturu menu a formuláře (zpočátku mi přišlo nepřirozené). Jako každý program, tak i zde byly zjištěny nedostatky - vyhledávání podle čísla nutno zadávat i x nul před číslem nebo jinak program záznam nenajde. Také mě překvapilo hodně zkratek, které jsem nerozluštil. Po dohodě s příručkou by asi nebyl problém. Program nabízí statistiky ISPV, ISP.

Mzdy 2008

Personální agenda

Postačující množství evidovaných údajů o zaměstnanci. Chybí personální agenda manželky a dětí. Daňové slevy a nezdanitelné částky nutno zadat ručně do seznamu, který se uchovává pro další zpracování.

Mzdová agenda

Mzdových údajů je menší množství, ale pro výpočet dostačující. Evidence nepřítomnosti, srážek, historie mezd, apod. Obsahuje evidenční listy důchodového pojištění a přihlášky k nemocenskému pojištění.

Hodnocení

Program bych po vizuální stránce hodnotil kladně. Menu je dobře pochopitelné. Program obsahuje obstojné množství tiskových sestav. Formuláře jsou dobře řešené. Pro laika jako velký přínos bych označil nepoužívání zkratek ve formulářích a dostatečně čitelné a strukturované formuláře.

OK mzdy

Personální agenda

Personální agenda obsahuje údaje pouze o zaměstnanci. Možnost evidování pracovního poměru. Možnost evidence turnusových úvazků. Možnost zadat odpočty na dani ke každému pracovníku.

Mzdová agenda

Evidování mzdových údajů. Evidence nepřítomnosti, srážek, historie mezd, apod. Možnost zadávání mzdových listů – počet odpracovaných hodin a minut v jednotlivých dnech. Není možnost zadávat, na čem daný pracovník pracoval. Zadávání měsíčních hodnot a hodnot pro daň a pojištění (např. zálohovou daň).

Hodnocení

Program po stránce ovládání mi přijde složitý. I po delší době proklikávání jsem nevěděl pořádně, co kde je a co to je. Přijde mi, že program je až moc členěn do mnoho obrazovek. Program má více menu (když počítáme různé záložky). Dále program obsahuje více ikonek, které nejsou na jednom místě.

Varia

Varia je program pro vedení kompletního účetnictví (podvojné účetnictví i daňová evidence). Vzhledem k obsahu diplomové práce se budu zabývat pouze mzdovou částí.

Personální agenda

Postačující množství evidovaných údajů o zaměstnanci. Možnost doplnění fotkou a popisem. Chybí personální agenda manželky a dětí. Daňové slevy a nezdanitelné částky nutno zadat ručně do seznamu u mzdové agendy, který se uchovává pro další zpracování.

Mzdová agenda

Mzdových údajů je menší množství, ale pro výpočet nejspíš dostačující. Mzdové údaje se zadávají v personální agendě. Uživatel může vybrat pracovní poměr, ale nenašel jsem možnost výběru typu mzdy. Evidence nepřítomnosti je evidována samostatně.

Hodnocení

Program bych po vizuální stránce obsahu a vzhledu hodnotil kladně. V menu programu se dá dobře vyznat a je zřejmé, co kde najít a která věc co znamená. Program nabízí množství tiskových sestav. Program nabízí roční zúčtovaní daně, potvrzení o zdaněných příjmech, evidence listů důchodového pojištění, ISPV, roční uzávěrku mezd, apod.

PC mzdy

Personální agenda

Neměl jsem možnost otestovat.

Mzdová agenda

Neměl jsem možnost otestovat.

Hodnocení

Program bych po vizuální stránce hodnotil záporně. První seznámení s programem, který disponuje DOSovským prostředím mě v dnešní době odrazuje.

PAMICA

Personální agenda

Evidování údajů o zaměstnanci včetně zdravotního, životního pojištění a penzijního připojištění. Neeviduje se manžel/manželka ani děti. Je zde možnost definování složek mezd (různé druhy mezd) a možnost zadávání nepřítomnosti zaměstnanců.

Mzdová agenda

V mzdové agendě je možnost pro zaměstnance definovat pracovní poměr a dovolenou. Definování údajů pro odpočet na dani nebo srážky jsem dlouho nemohl najít. Chybí možnost evidence mzdových listů. Možnost elektronického podání PVS a ELPD. exportů hlášení pro jednotlivé pojišťovny a přihlášky/odhlášky pro ČSSZ. Program nabízí výpočet hrubé a čisté mzdy.

Hodnocení

I přes kvalitní zpracování menu jsem některé části programů nemohl najít. Menu mi přijde až moc stručné a nejde se dostat přes něj tam, kde člověk potřebuje. Dlouho mi trvalo, než jsem se v tomto programu začal orientovat. Pro další spolupráci bych musel asi často používat nápovědu. V demoverzi je následně další omezení na vystavení mezd jen na březen a duben roku 2008 a tímto se mi nepodařilo ani testovací vystavení mezd. Po delším seznámení by snad s programem nebyl další problém.

MoneyS3

Demoverze, kterou jsem měl stáhnutou, obsahovala kompletní účetnictví. V této části budu popisovat jen část programů zadívající se mzdami.

Personální agenda

Dostatečná množství evidovaných údajů. Personální evidence manželky a dětí chybí. Možno pro každého zaměstnance definovat příplatky za určitých podmínek. K osobě tento program nabízí přiřazení osobního automobilu. Dále je také možnost k osobě poznamenat si další poznámky.

I při personální agendě dětí nutnost vložit počet dětí pro slevu na dani. Možnost evidence cizinců a také možnost v personální agendě dopsat další text pro každou osobu. Možnost vložení fotky. Kvalitní vyhledávání a sestavy podle různých atributů. Dále agenda školení a kurzů, příspěvky a dary, exekuce, stalé srážky a nemocenské dávky.

Mzdová agenda

Sleva na dani se udává při definování personální agendy. Měsíční slevy na dani/nezdanitelné částky se zadává do kolonek ve vypočtené výši. Dále pro výpočet mezd se zadávají informace o

odpracovaných údajích, o hrubé mzdě, nemocenské dávce, vyúčtování zaměstnanec a zaměstnavatel. Je možné definovat pracovní poměry, svátky, nové příplatky, apod.

Hodnocení

Program bych hodnotil kladně. V programu se dá dobře orientovat a program se dobře člení na jednotlivé sekce. Program disponuje celou řadu tiskových sestav pro výstup dat. Dále je možnost zaúčtování záloh a zaúčtování mezd do účetního systému Money S3. Formuláře jsou dobře členěný. Popisky jednotlivých položek jsou taktéž dobře srozumitelné.

Účto

Hodnocení

Jedná se stejně jako u systému PC mzdy o DOSovské prostředí. Proto základní hodnocení vzhledu bych hodnotil záporně. Tento systém je však široce rozšířen, a proto je ho třeba zařadit mezi programy obsahující výpočet mezd.

B. Autentizace, autorizace a bezpečnost

Na platformě .NET

Pro autentizaci na platformě .NET jsem vycházel z těchto zdrojů [44], [45] a [46] uvedených v oddílu literatura a informační zdroje.

Na platformě .NET je implementováno řízení přístupu na základě uživatelských rolí. Jednotliví uživatele jsou přiřazeni do jednotlivých rolí. Každý uživatel může být přiřazen do více rolí a podle role je následně prováděna autorizace. Na začátku vývoje aplikace se definují role a jejich funkcionalita a následně se přiřazují uživatele do těchto rolí. Realizace na platformě .NET by šlo rozdělit do dvou skupin, a to za prvé stolních .NET aplikací a webových .NET aplikací. Následně se zaměřím na webové aplikace.

Informace o tom, že uživatel je přiřazen do určité role je obsaženo v objektech typu *principal*. Objekty musí dědit z rozhraní *IPrincipal*, které obsahují referenci na uživatele a obsahují metodu *IsInRole*, která nám umožňuje ověření rolí.

Ve webovém prostředí ASP.NET běžící aplikace má svůj vlastní bezpečnostní kontext. Na rozdíl od vláken při stolní aplikaci je *principal* uložen v proměnné *User* aktuálního kontextu *HttpContext (System.Web.HttpContext.User)*. IIS, na kterém běží pracovní proces ASP.NET, využívá uživatelské účty operačního systému a podporuje různé druhy autentizace. Tedy autentizaci pomocí zasílání uživatelského jména a hesla, autentizace v lokální síti, zasílání certifikátu v http požadavku, podle kterého se vybere odpovídající uživatelský účet.

Autentizace v prostředí ASP.NET může být realizována třemi způsoby. Pokud má každý uživatel (který bude využívat aspx aplikaci) v lokální síti účet, může se přihlásit pomocí něj. Tedy první možnost je nechat autentizaci na starost IIS serveru tzv. *Windows autentizace*. Za druhé můžeme využít autentizaci pomocí *Forms autentizace*. U Forms musíme práci spojenou s přihlášením uživatele udělat sami v aspx aplikaci. Většinou jsou jména a hesla uživatelů uložena v rámci aplikace (zpravidla v relační databázi). Pro *Forms autentizaci* je nutné první vytvořit tabulku v databázi a vložit do ní data o účtech uživatelů. Pro tuto úlohu je k dispozici konfigurační nástroj. Další možnost je využít službu *Microsoft .Net Passport*. U této autentizace je nutné zajistit určitou kvalitu aplikace. Aplikace musí například zajistit ochranu osobních dat, čištění po odhlášení a podobně.

Autorizace v ASP.NET závisí na použitém autentizačním modelu. Při využití windows uživatelských účtů, na kterých může běžet ASP.NET proces, můžeme využít jednoduchou autorizaci, kterou poskytuje souborový systém. Specifikace přístupových práv se provádí v souboru *web.config* v adresáři aplikace. Zde se nastavuje taky způsob autentizace. Můžeme povolovat nebo zakazovat různé role, ale také http požadavky jako je POST a GET. U *Forms autentizace* se také vytváří souborová struktura, kde se nastavuje oprávnění k přístupu ke složkám. Nastavení se provádí zas ve *web.config* souborech.

Kryptografie na platformě .NET

Třídy pro kryptografii se na platformě .NET nachází v jmeném prostoru *System.Security.Cryptography*. Symetrické algoritmy jsou implementovány v třídách, které dědí z abstraktní třídy *SymmetricAlgorithm*. Algoritmy pracují s bloky dat pevné délky (CBC – Cipher Block Chaining). Základní třídu pro hashovací algoritmy tvoří *HashAlgorithm*. Tato třída následně obsahuje tři přetížené metody pro vytváření hashe. Dále platforma poskytuje podporu pro digitální certifikáty ve formátu *X.509*. Jmenný prostor je *System.Security.Cryptography.X509Certificates*. Od frameworku verze .NET 2.0 je k dispozici také třída *X509Certificate2*, která nově podporuje také CRL(Certificate Revocation List). Dále je zde třída pro bezpečné náhodné generování čísel – *RandomNumberGenerator*.

Na platformě Java

Pro autentizaci na platformě Java jsem vycházel z těchto zdrojů [46], [47] a [48] uvedených v oddílu literatura a informační zdroje.

Na platformě java existuje služba Java Autentication and Authorization Service (JAAS). Původně služba byla volně šiřitelná, ale po čase došlo k k začlenění přímo do platformy. JAAS lze použít pro dva účely:

- pro autentikaci uživatelů, neboli pro spolehlivé a bezpečné určení toho, kdo právě spouští Javový program (kód aplikace, aplet, Java bean, servlet)
- pro autorizaci uživatelů zdali mají přístupová práva k provedení požadované akce

Architektura autentizační části je postavena na principu plugin – implementována Javovská verze standardního systémového *Pluggable Authentication Modulu* (PAM). Tedy je rozšiřitelná o připojitelné moduly implementující různé možnosti autentizace (např. RSA, DCE, Kerberos, …). Tedy není nutné měnit aplikaci, pokud chceme používat nové možnosti autentizace. Stačí přídat nebo aktualizovat do systému nový plugin.

Pokud aplikace potřebuje nějakou formu autentizace, vyvolá nejdříve objekt *LoginContext*, který se odkazuje na vlastnost *Configuration*. V konfiguraci je uvedeno, který přihlašovací modul (objekt LoginModule) se má vyvolat a v jakém prostředí. V ní jsou uvedeny způsoby, kterými si aplikace ověří, kdo ji spouští. Pokud byli uživatel nebo služba autentizováni, přichází na řadu autorizační komponenta JAAS.

Popis základních tříd a rozhraní

Společné třídy:

- *Subject* – zdroj, kdo požaduje na práci s chráněným zdrojem (uživatel, jiná služba). Po autentikaci je jeho identita určená *Principalem. Subject* může mít pro různé služby různé *Principaly*
- *Principals* – reprezentuje identitu subjektu (je asociován pokud byla autentikace úspěšná)
- *Credentials* – doplňková data bezpečnostního charateru

Autentikační třídy a rozhraní:

- LoginContext – poskytuje základní metody používané k autentikaci uživatelů. Zjišťuje informace s objektu *Configuration* aby určil druh autentikačních služeb a potřebné LoginModuly. Obsahuje metody např.: *login*, *getSubject*, *logout*
- *LoginModule* – rozhraní implementující různé typy autentikačních mechanismů (např. modul pro přihlášení jménem a heslem nebo pro biometrické přihlášení)
- *CallbackHandler* – rozhraní pro komunikaci s uživatelem po získání autentizacích informací
- *Callback* – rozhraní které mohou LoginModuly vracet metodám *CallbackHandleru*

Autorizační třídy:

- *Policy* – abstraktní třída pro implementaci systémové přístupové politiky. Podporuje *Principals*
- *AuthPermission* – zapouzdřuje základní přístupová práva v JAAS (čtení, zápis, …)
- *PivateCredentialPermission* – chrání soukromé *Credentials* a obsahuje metodu řídicí přístupu k těmto privátním informacím

Kryptografie na platformě JAVA

V platformě Java je kryptografie podporována pomocí *Java Cryptography Architecture* (JCA). Tato součást platformy obsahuje systém poskytovatelů kryptografických služeb a aplikačního programovacího rozhraní pro symetrické i asymetrické šifry, hashe, digitální podpisy, certifikáty, tvorbu klíčů a náhodné generátory. JCA nespoléhá na žádné kryptografické služby operačního systému.

Základní třídou pro poskytovatele je *java.security.Provider*, která obsahuje názvy poskytovatelů a především seznam všech služeb, které nabízí. Pak na základě žádosti dokáže JCA nalézt správnou třídu. Různé verze JDK mohou obsahovat různé typy providerů. Proto by neměl programátor spoléhat na to, že provider bude vždy k dispozici.

Poznámka k obrázku: Aplikace požaduje instanci třídy AES (symetrická šifra). JCA musí nalézt poskytovatele, který podporuje tuto šifru (CSP3). Následně poskytovatel vrací instanci své třídy *com.foo.AESCipher*, což je potomek *CipherSpi*, a ta je zabalena v nově vytvořené instanci *javax.crypto.Cipher*, která je vrácena aplikaci.

Podpora PKI je na platformě Java obsažena v jmenném prostoru *java.security.cert*. Jako úložiště řetězce certifikátů obsažené v binárních souborech, může být třeba LDAP. Pro binární proud obsahující certifikáty, použijeme třídu *CertificateFactory*. Informace v něm obsažené reprezentuje instance třídy *CertPath*. JCA provider SUN podporuje certifikáty ve formátu X.509 a kódování PKCS#7. Java podporuje také rozhraní pro správu klíčů a certifikátů v databázích zvaných *keystore*. Pro přístup do *Kastore* slouží instance třídy *java.security.KeyStore*.

Seznam JCA providerů a šifrovacích algoritmů od společnosti Sun jsou na adrese: http://java.sun.com/javase/6/docs/technotes/guides/security/SunProviders.html.

Na platformě PHP

Pro autentizaci na platformě PHP jsem vycházel z těchto zdrojů [49], [50], [51], [52] a [53] uvedených v oddílu literatura a informační zdroje.

V PHP máme dvě možnosti autentizace pomocí jména a hesla. První je využití možnosti protokolu http. S pomocí odezvy *401 Unauthorized* a následně hlavičky *WWW-Authenticate* sdělí server klientovi, že potřebuje přihlašovací údaje. Ověření údajů lze provést na úrovní aplikace nebo na úrovni webového serveru. U Apache toto zajišťují moduly *mod_auth, mod_auth_db a mod_auth_dbm*. Tato autentizace má několik nevýhod. Práce je málo pohodlná a zabezpečovací údaje putují sítí při každém požadavku (lze eliminovat šifrovaným přenosem či použití HTTP Digest autentizace). Největší problém spočívá k donucení klienta k odhlášení.

Druhý způsob autentizace je tzv. formulářová. Aplikace v případě potřeby zašle klientovi stránku s přihlašovacím HTML formulářem. Po úspěšném přihlášení je uživatel spojen v aktuálním session. Dále při komunikaci se už předává pouze token a server má možnost kdykoliv klienta odhlásit (např. vypršení timeout).

Zobecnění v oblasti jazyka PHP pro autentizaci (aby nebylo chybně vymyšlená pro každý projekt) může být například knihovna PEAR. Tato knihovna obsahuje obecnou třídu *Auth* a pro autentizaci založenou na HTTP zvláštní třídu *Auth_HTTP*.

Pro správu uživatelů a uživatelských skupin (neboli role), autentizaci, správu přístupových práv a podobně je vhodné využít nějaký framework. Pro zajištění těchto potřeb můžeme využít například aplikační framework phpBASE. V termilogii MVC je phpBASE postavený na centrálním Font Controlleru (tedy přijímá a zpracovává všechny požadavky od uživatelů zpravidla na jednom jediném URL).

Kryptografie na platformě PHP

Pro šifrování v PHP máme knihovny *krypt* nebo *mhash*. Tyto knihovny obsahují celou řadu algoritmů. Např. knihovna *mcrypt* obsahuje:

MCRYPT_3DES, MCRYPT_DES, MCRYPT_TripleDES, MCRYPT_ENIGMA, MCRYPT_IDEA, MCRYPT_RIJNDAEL_256, MCRYPT_RC6, MCRYPT_SAFER+28, MCRYPT_SERPENT_256, MCRYPT_THREEWAY, MCRYPT_TWOFISH256, …

Bohužel asi mnohé s těchto algoritmů nejsou dostatečně bezpečné. K použití algoritmů můžeme využít funkce z *mcrypt*. Před použitím musíme znát algoritmus kódování, který chceme použít, režim, ve kterém chceme kódovat a konstantu, která udává, co chceme s daným řetězcem dělat. Režimy mohou být např.: EBC, CBC, OFB, NOFB, STREAM, … a konstanty MCRYPT_ENCRYPT, MCRYPT_DECRYPT, MCRYPT_DEV_RANDOM, MCRYPT_DEV_UNRANDOM, MCRYPT_RAND.

Na platformě Oracle

Pro autentizaci na platformě Oracle jsem vycházel z těchto zdrojů [27] a [54] uvedených v oddílu literatura a informační zdroje.

Pro popis bezpečnosti na této platformě byl využít aplikační server Oracle10g. Tento aplikační server nám poskytuje IDE prostředí pro vývoj, správu a distribuci internetových aplikací s názvem Oracle10g APEX[153] (Oracle Application Express). Toto vývojové prostředí spolupracuje především s prostředím databázi Oracle10g. Jedná se o prostředí, kde se skoro obejdete bez programování.

Bezpečnost

Oracle database poskytuje širokou škálu bezpečnostních mechanismů, např. v oblasti řízení přístupu, šifrování či auditování, které ji předurčují pro použití i v prostředích s vysokými nároky na bezpečnost. Důvěryhodnost implementace těchto mechanismů dokazuje i mnoho nezávislých bezpečnostních ohodnocení. Výhoda těchto zabezpečení je zajištění na úrovní databázového serveru. Výhody, které z tohoto plynou oproti zabezpečení na úrovni aplikace jsou:

- Pokud k datům přistupuje více aplikací jsou práva definována centrálně a není potřeba je implementovat v každé aplikaci. Za důsledek to má vetší efektivitu a snížení rizika, že nějaká implementace nebude dostatečně kvalitní.

[153] APEX – Oracle Application Express

- Řízení přístupu a řada dalších bezpečnostních mechanismů je převážně deklarativní, nevyžaduje programování. Tedy lze pomocí systémových protokolů kontrolovat správné nastavení a není potřeba se vyznat v programování.
- Minimalizace ohrožení dat v případě kdy útočník získá kontrolu nad aplikací. Např. škody napadení pomocí SQL Injection můžou být nulové nebo minimální, pokud aplikace přistupuje k databázi přes uživatele s minimálními právy.
- Oracle prošel řadou nezávislých bezpečnostních certifikací (zde např. ISO 15408 na úrovni EAL-4, tedy Common Criteria for Information Technology Security Evaluation).

Řízení přístupu

Databáze nabízí řadu různých odstupňovaných systémových i objektových přístupových práv. To nám zajišťuje možnost, jak přidělovat každému uživateli pouze minimální nutná práva. Je všeobecně známo, že každé právo navíc zvyšuje riziko zneužití. V databází Oracle najdete klasický systém rolí. Tedy pro skupinu lidí nemusíme procházet dlouhý seznam a přidělovat práva, ale stačí přidělit roli.

V databázovém systému lze taky přidělit práva pouze na přístupu z konkrétní aplikace – **Secure Application Role**. Tyto role jsou pevně svázány s určitou databázovou package (knihovnou uložených procedur) a mohou být aktivovány pouze s této package. V dané package lze provést dodatečné kontroly a aktivovat roli jen na základě splnění podmínek.

Dalším z problému řešených v Oracle je, jak zařídit přístup uživateli z různých oddělení pouze ke svým datům. Může se stát, že data celého podniku jsou ve stejné tabulce. Pro tyto účely bylo do Oracle doimplementováno řízení přístupu na úrovni záznamů – **Virtual Private Database** (VPD). VPD zajišťuje doplnění databázového dotazu o bezpečnostní podmínku.

Další vlastnost implementovanou do databáze Oracle je mechanismus důvěrnosti – **Oracle Label Security Option**. Každý záznam je označen štítkem označující jeho citlivost. Následně každý uživatel má definovány bezpečnostní úrovně, se kterými může pracovat.

Identifikace a autentifikace uživatele

Základním mechanismem implementováním v Oracle je autentifikace pomocí jména a hesla. Dále je zde rozšíření o různé pokročilé metody implementované rámci **Oracle Advenced Security Option** (ASO). Zde lze zahrnout klientské SSL certifikáty, a další autentifikační služby postavené na standardech Kerberos či RADIUS. Pomocí těchto služeb lze zajistit ověřování například pomocí biometrických údajů nebo různých elektronických karet.

U webových aplikací může nastat problém s identifikací uživatelů a to díky technologií, kdy se aplikace do databáze přihlašuje stále pod stejným jménem a heslem. Databáze tedy nepozná, kdo s ní v daném okamžiku pracuje, což blokuje řadu jejich bezpečnostních funkcí. Z tohoto důvodu bylo doimplementováno **Proxy Authentication**. Aplikace stejně stále přistupuje pod stejným jménem a heslem a ušetří tak čas na vytváření spojení, avšak nám umožňuje předat informace o skutečném uživateli, který s aplikací zrovna pracuje. Databázový systém to následně využívá při řízení přístupu.

Šifrování

Šifrování nám umožňuje zabránit odposlechu či pozměnění dat při přenosu komunikace. V Oracle lze použít šifrování pomocí SSL a lze použít i další algoritmy obsažené v rámci **Advanced Security Option**. Šifrování komunikace je transparentní pro aplikaci. Zavedení šifrování je otázkou konfigurace a není potřeba zasahovat do zdrojového kódu aplikace. Dále lze vybrat programové šifrování a dešifrování dat pomocí algoritmů, jako je DES, 3DES, AES a MD5. Vetšinou nám slouží pro šifrování citlivých dat. Advenced Security Option byla ve verzi Oracle10g Release 2 rozšířena o šifrování dat v tabulkách. Toto šifrování je transparentní z pohledu aplikace. Tento mechanismus chrání před únikem dat, například kopírováním datových souborů nebo zcizení záložních medií s daty.

Audit operací

Systém nám nabízí bezpečnostní mechanismus, který nám umožňuje auditovaní operací prováděných jednotlivými uživateli. Pro procházení velkého množství záznamů, Oracle implementoval **Fine Grained Auditing** (FGA). FGA umožňuje určit jakých dat se má operace týkat, specifikaci sloupce tabulky a podmínky. Při definované události je možno například poslat SMS správci databáze.

Správa uživatelů

V oracle je takzvaná centrální správa uživatelů. Správa uživatelů se provádí na jenom místě, ze kterého si jednotlivé aplikace přebírají data pomocí standardu LDAP. V Oracle pro centrální správu byl implementován **Oracle Internet Directory** (OID). OID lze samozřejmě využít i pro správu databázových uživatelů a rolí. Tato funkcionalita je označována jako **Enterprise User Security**.